기록의 양면성 원리 원천 개념 정의서
신뢰를 만드는 기록과 위험을 만드는 기록

문서 기본 정보

작성자: 노태윤
작성일: 2026년 5월 8일
문서 유형: 원천 개념 정의서 / 원천 철학 문서 / 신뢰 기술 개념 문서
핵심 주제: 기록, 신뢰, 사생활, 보안, 검증, 권한, 인공지능, 디지털 문명
문서 목적: 아카이브 등록 및 공개 기록
연결 개념: 믿집, Trust Score, DET, 디지털 실존 증명, 신뢰 기록 최소화 원칙, AI 신뢰 판단 보조
범위 설명: 본 문서에서 말하는 기록은 문서에 한정되지 않으며, 텍스트, 대화, 이미지, 음성, 영상, 접속 로그, 전자서명, 시스템 출력값, 판단 결과, AI 생성물 등 인간의 행위와 상태가 남긴 다양한 형태의 기록물을 포함한다.

본 문서는 기술 구현 명세서가 아니라, 디지털 사회에서 기록이 신뢰와 위험으로 분화되는 구조를 정의하고, 미래 신뢰 기술이 따라야 할 철학적 방향을 정리한 원천 개념 정의서이다.

1. 문제의식과 제안 배경

1.1 기술과 문명의 발전은 왜 기록을 증가시키는가

기술과 문명이 발전할수록 인간의 행위는 더 많이 기록된다.

과거의 기록은 제한적이었다. 계약은 종이에 남았고, 거래는 장부에 남았으며, 약속과 관계는 사람들의 기억 속에 남았다. 기록은 물리적 공간과 시간의 제약을 받았고, 기록할 수 있는 행위도 제한되어 있었다.

그러나 디지털 사회에서는 거의 모든 행위가 기록될 수 있다. 사람이 어디에 접속했는지, 무엇을 구매했는지, 누구와 대화했는지, 어떤 문서를 열람했는지, 어떤 선택을 했는지, 어떤 정보를 확인했는지까지 데이터로 남을 수 있다.

기술은 편리함을 위해 기록을 만든다. 서비스는 사용자의 이력을 기억해야 더 편리해지고, 플랫폼은 거래 내역을 남겨야 분쟁을 줄일 수 있으며, 보안 시스템은 접속 기록을 남겨야 이상 행위를 탐지할 수 있다.

문명은 책임을 위해 기록을 만든다. 계약의 책임, 거래의 책임, 행위의 책임, 승인과 거절의 책임을 남기기 위해 기록은 필요하다.
따라서 디지털 사회에서 기록의 증가는 우연이 아니다. 그것은 편리함, 효율성, 책임성, 보안, 검증 가능성을 요구하는 문명의 자연스러운 흐름이다.
기록은 문명이 더 복잡해질수록 증가한다.
사람과 사람 사이의 약속이 늘어나고, 기관과 개인 사이의 거래가 늘어나고, 플랫폼과 사용자의 상호작용이 늘어날수록 사회는 더 많은 근거를 필요로 한다.
기록은 그 근거의 형태다.
그러나 기록이 증가한다는 것은 신뢰의 가능성이 커진다는 뜻이면서, 동시에 위험의 가능성도 커진다는 뜻이다. 더 많은 기록은 더 많은 증거를 만들지만, 더 많은 노출과 더 많은 감시의 가능성도 만든다.
이 지점에서 기록의 양면성 문제가 시작된다.
1.2 계약, 거래, 인증, 대화, 창작, 접속 기록의 확대
디지털 사회에서 기록은 특정 영역에만 머물지 않는다.
계약은 전자계약으로 남고, 거래는 결제 기록과 송금 기록으로 남는다. 인증은 로그인 기록과 전자서명 기록으로 남으며, 대화는 메신저와 이메일, 음성, 영상 기록으로 남을 수 있다.
창작물은 업로드 시점, 수정 이력, 원본 파일, 생성 경로, 출처 정보와 함께 기록된다. 접속 기록은 사용자가 언제 어디에서 어떤 시스템에 접근했는지를 남긴다.
이처럼 인간의 행위는 점점 더 세밀하게 기록된다.
기록은 더 이상 특별한 사건에만 남는 것이 아니다. 일상의 선택, 습관, 관계, 판단, 이동, 소비, 대화까지 기록의 대상이 될 수 있다.
이 변화는 사회를 더 투명하게 만들 수 있다. 그러나 동시에 개인의 삶을 과도하게 노출시킬 수도 있다.
기록이 많아진다는 것은 증거가 많아진다는 뜻이기도 하지만, 노출될 수 있는 약점이 많아진다는 뜻이기도 하다.
계약 기록은 분쟁을 줄일 수 있지만, 개인의 재산 상태와 거주 정보를 노출시킬 수 있다. 거래 기록은 사기를 추적할 수 있지만, 개인의 경제적 취약성을 드러낼 수 있다. 인증 기록은 보안을 강화할 수 있지만, 사용자의 행동 패턴을 감시하는 근거가 될 수 있다.
대화 기록은 피해자의 증거가 될 수 있지만, 맥락 없이 공개되면 개인을 공격하는 도구가 될 수 있다. 창작 기록은 저작권과 출처를 보호할 수 있지만, 동

시에 창작자의 작업 과정과 사적 흔적을 과도하게 노출할 수 있다.
따라서 기록의 확대는 단순한 기술 발전의 문제가 아니다.
그것은 인간의 삶이 점점 더 많은 데이터와 연결되는 문명적 변화다.
이 변화 속에서 중요한 질문은 “얼마나 더 많이 기록할 것인가”가 아니다.
중요한 질문은 “무엇을 기록하고, 무엇을 보호하며, 필요한 순간에 무엇만 검증할 것인가”이다.

1.3 기록이 신뢰의 기반이 되는 이유

기록은 신뢰의 기반이 될 수 있다.
기록이 있기 때문에 사람은 말이 아니라 근거로 판단할 수 있다. 계약서가 있으면 계약 내용을 확인할 수 있고, 거래 내역이 있으면 돈의 흐름을 추적할 수 있다. 인증 기록이 있으면 누가 어떤 권한으로 접근했는지 확인할 수 있고, 승인 기록이 있으면 어떤 행위가 실제로 허가되었는지 확인할 수 있다.
기록은 책임을 만든다.
기록은 “그런 적 없다”는 부정을 줄이고, “언제, 누가, 무엇을, 어떤 조건에서 했는가”를 확인하게 한다.
기록은 약자를 보호할 수 있다.
말로만 이루어진 관계에서는 힘이 강한 사람이 유리할 수 있다. 그러나 기록이 있으면 피해자는 자신의 상황을 증명할 수 있다.
기록은 사기와 조작을 줄일 수 있다.
기록이 남는다는 사실은 부정행위를 억제하고, 문제가 발생했을 때 원인을 추적할 수 있게 한다.
이 점에서 기록은 문명의 방패다.
기록은 사회가 신뢰를 만들고 유지하기 위한 중요한 기반이다. 기록이 없다면 사회는 기억, 주장, 권위, 힘의 관계에 의존해야 한다. 그러나 기록이 있으면 판단은 조금 더 근거에 가까워진다.
기록은 인간 사회에 세 가지 신뢰 기능을 제공한다.
첫째, 행위의 존재를 확인하게 한다.
어떤 일이 실제로 있었는지, 어떤 약속이 이루어졌는지, 어떤 거래가 발생했는지 확인할 수 있다.
둘째, 행위의 주체를 확인하게 한다.
누가 승인했는지, 누가 접근했는지, 누가 계약했는지, 누가 변경했는지를 확인할 수 있다.
셋째, 행위의 책임을 확인하게 한다.
문제가 발생했을 때 책임이 어디에 있는지 추적할 수 있다.

이러한 기능 때문에 기록은 신뢰의 기반이 된다.
그러나 기록이 신뢰가 되기 위해서는 조건이 필요하다. 기록은 정당한 권한, 적절한 목적, 안전한 보호 구조, 검증 가능한 무결성 안에서 다루어져야 한다.
기록이 보호 구조 없이 남겨질 때, 그 기록은 신뢰가 아니라 위험이 될 수 있다.
1.4 기록이 사생활 침해와 감시의 도구가 되는 이유
그러나 기록은 동시에 사생활 침해와 감시의 도구가 될 수 있다.
기록은 사람을 보호할 수도 있지만, 사람을 노출시킬 수도 있다. 개인의 위치, 대화, 건강, 재산, 관계, 소비, 감정, 실수, 약점이 기록되고 공개되면, 그 기록은 개인의 삶을 무너뜨리는 무기가 될 수 있다.
기록이 권한 없이 수집되면 사생활 침해가 된다. 기록이 권력이나 플랫폼에 집중되면 감시가 된다. 기록이 악의적인 사람에게 넘어가면 협박과 조작의 도구가 된다.
기록은 그 자체로 중립적일 수 있다. 그러나 누가, 어떤 권한으로, 어떤 목적을 위해, 어느 범위까지 기록을 보는가에 따라 기록의 의미는 완전히 달라진다.
문제는 기록이 많아지는 것 자체만이 아니다. 문제는 기록을 다루는 권한과 통제 구조가 기록의 증가 속도를 따라가지 못하는 데 있다.
기록이 신뢰가 되려면 보호 구조가 있어야 한다.
보호 구조 없는 기록은 신뢰가 아니라 위험이 될 수 있다.
사생활 침해는 기록이 개인의 통제 범위를 벗어날 때 발생한다. 사람이 어떤 정보를 누구에게 보여줄지 선택할 수 없고, 자신의 기록이 어디에 저장되고 어떻게 활용되는지 알 수 없다면, 기록은 개인의 삶에 대한 통제권을 빼앗는다.
감시는 기록이 지속적으로 수집되고 분석될 때 발생한다. 모든 행위가 기록되고, 그 기록이 평가와 예측의 대상이 되면 사람은 자유롭게 말하고 행동하기 어려워진다.
기록이 많아질수록 사람은 스스로를 검열할 수 있다.
무엇을 말해도 기록될 수 있고, 어떤 선택도 평가될 수 있으며, 과거의 실수도 영구적으로 남을 수 있다는 감각은 인간의 자유를 위축시킨다.
따라서 기록은 인간을 보호하기 위해 존재해야지, 인간을 감시하고 통제하기 위해 존재해서는 안 된다.
이것이 기록 사회에서 가장 중요한 윤리적 기준이다.
1.5 기록 사회에서 발생하는 새로운 위험
기록 사회에서는 새로운 위험이 발생한다.

첫째, 사생활 노출 위험이다.
개인의 일상, 관계, 감정, 실수, 건강, 금융 정보가 공개될 경우 그 피해는 단순한 불편을 넘어 삶 전체에 영향을 줄 수 있다.
둘째, 비밀 기록 유출 위험이다.
조직 내부 문서, 계약 정보, 연구 자료, 전략 자료, 고객 정보가 유출되면 개인뿐 아니라 조직과 사회에도 피해가 발생할 수 있다.
셋째, 감시와 통제 위험이다.
모든 행동이 기록되고 평가되는 사회에서는 사람의 자유가 위축될 수 있다. 인간은 실수하고 회복해야 하지만, 기록이 영구적으로 남으면 회복의 기회가 줄어들 수 있다.
넷째, 기록 조작 위험이다.
기록은 진실을 보여줄 수 있지만, 일부만 편집된 기록은 거짓을 진실처럼 보이게 만들 수도 있다.
다섯째, 범죄 모의와 악용 위험이다.
기록은 범죄를 추적하는 도구가 될 수 있지만, 동시에 범죄자가 누군가의 습관, 위치, 자산, 관계, 취약점을 파악하는 자료가 될 수도 있다.
여섯째, 기록 과잉의 위험이다.
모든 것을 저장하는 사회는 반드시 안전한 사회가 아니다. 오히려 과도한 기록은 새로운 유출 위험과 감시 위험을 만든다.
일곱째, AI 기반 추론 위험이다.
인공지능은 여러 기록을 결합해 개인이 직접 공개하지 않은 정보까지 추론할 수 있다. 검색 기록, 소비 기록, 대화 기록, 위치 기록, 금융 기록이 결합되면 개인의 성향, 불안, 경제적 취약성, 관계 상태, 생활 패턴까지 추론될 수 있다.
여덟째, 허위 기록 생성 위험이다.
AI는 실제처럼 보이는 문서, 이미지, 음성, 영상, 대화 기록을 생성할 수 있다. 이로 인해 무엇이 실제 기록이고 무엇이 조작된 기록인지 구분하기 어려워질 수 있다.
따라서 기록 사회의 핵심 문제는 단순히 저장 용량이나 기술 수준의 문제가 아니다.
핵심은 기록의 권한, 목적, 범위, 보호, 검증 구조를 어떻게 설계할 것인가이다.
기록 사회의 위험은 기록의 부족에서만 오는 것이 아니다.
이제 위험은 기록의 과잉, 기록의 유출, 기록의 조작, 기록의 추론, 기록의 생성에서도 발생한다.

이 변화는 기록을 다루는 철학을 새롭게 요구한다.

1.6 왜 지금 기록의 방향을 다시 정의해야 하는가

지금 기록의 방향을 다시 정의해야 하는 이유는 명확하다.

디지털 사회는 이미 기록 사회로 진입했다. AI, 전자계약, 플랫폼, 디지털 신원, 블록체인, 공공데이터, 보안 인증, 자동화 시스템은 모두 기록을 기반으로 작동한다.

그러나 기록이 증가하는 속도에 비해, 기록을 안전하게 다루는 철학과 원칙은 충분히 정리되어 있지 않다.

많은 기술은 더 많이 저장하고, 더 많이 분석하고, 더 많이 연결하는 방향으로 발전한다. 그러나 미래의 신뢰 기술은 단순히 더 많은 데이터를 모으는 방향만으로는 충분하지 않다.

앞으로 필요한 것은 더 많은 기록이 아니라, 더 안전한 기록이다.

더 많은 저장이 아니라, 더 정교한 권한과 검증이다.

더 많은 공개가 아니라, 필요한 사실만 증명하는 구조이다.

기록의 방향을 다시 정의하지 않으면, 신뢰를 만들기 위해 남긴 기록이 오히려 인간을 해치는 도구가 될 수 있다.

특히 인공지능의 발전은 이 문제를 더욱 시급하게 만든다. AI는 기록을 빠르게 분석하고, 숨겨진 패턴을 찾아내며, 인간이 보지 못한 위험 신호를 발견할 수 있다. 그러나 동시에 AI는 기록을 과도하게 해석하거나, 민감한 사실을 추론하거나, 허위 기록을 생성할 수 있다.

따라서 기록의 방향은 단순히 저장과 보관의 문제가 아니다.

기록은 해석되고, 판단되고, 생성되고, 검증되는 문제로 확장되었다.

이제 필요한 것은 기록의 새로운 원칙이다.

기록은 감시를 위해 존재해서는 안 된다.

기록은 보호를 위해 존재해야 한다.

기록은 사람을 통제하기 위해 존재해서는 안 된다.

기록은 사람이 위험을 피하고, 억울함을 줄이며, 스스로를 지킬 수 있도록 존재해야 한다.

이것이 본 문서가 기록의 방향을 다시 정의하려는 이유이다.

1.7 인공지능은 기록의 해석과 생성 방식을 바꾼다

인공지능의 발전은 기록의 의미를 더욱 확장시킨다.

과거의 기록은 사람이 직접 읽고 해석해야 하는 자료에 가까웠다. 계약서, 거래 내역, 대화 기록, 접속 기록, 인증 기록은 사람이나 기관이 필요할 때 확인하는 근거였다.

그러나 인공지능은 기록을 단순 보관물이 아니라 해석 가능한 신호로 바꾼다.
AI는 흩어진 기록을 분석하고, 요약하고, 분류하며, 위험 신호를 찾아내고, 미래의 가능성을 예측하는 데 활용될 수 있다. 계약서 문구에서 위험 조항을 찾고, 거래 기록에서 이상 패턴을 감지하며, 대화 기록에서 보이스피싱 신호를 탐지하고, 인증 기록에서 비정상 접근을 발견할 수 있다.
이 점에서 인공지능은 기록을 신뢰 판단으로 연결하는 강력한 도구가 될 수 있다.
그러나 인공지능은 기록의 위험도 함께 증폭시킨다.
AI는 기록을 바탕으로 개인의 성향, 취약점, 경제 상태, 심리 상태, 관계 구조를 추론할 수 있다. 또한 맥락이 부족한 기록을 과도하게 해석하거나, 편향된 판단을 만들거나, 조작된 이미지·음성·문서·대화와 같은 가짜 기록을 생성할 수도 있다.
따라서 AI 시대의 기록 문제는 단순히 “무엇을 저장할 것인가”의 문제가 아니다.
이제 기록의 문제는 “누가 기록을 해석하는가”, “어떤 기준으로 판단하는가”, “그 판단은 설명 가능한가”, “AI가 생성한 기록과 인간이 남긴 기록을 어떻게 구분할 것인가”의 문제로 확장된다.
인공지능은 기록을 신뢰로 바꿀 수 있다.
그러나 통제되지 않은 인공지능은 기록을 감시, 조작, 예측 통제, 허위 생성의 도구로 바꿀 수도 있다.
따라서 AI 기반 신뢰 기술은 반드시 기록 최소화, 원본 보호, 선택적 공개, 설명 가능한 판단, 사용자 통제권의 원칙 위에서 설계되어야 한다.
AI는 기록을 해석할 수 있다.
그러나 기록을 해석하는 권한은 인간 보호의 원칙 안에 있어야 한다.
AI는 신뢰 판단을 도울 수 있다.
그러나 AI가 인간의 삶을 감시하고 통제하는 최종 권한이 되어서는 안 된다.

2. 최초 핵심 명제

2.1 기록은 선도 악도 아니다
기록은 선도 악도 아니다.
기록은 인간의 행위가 남긴 흔적이며, 그 자체만으로 도덕적 성격을 갖지 않는다. 같은 기록이라도 어떤 목적과 권한, 구조 안에서 사용되는가에 따라 전혀

다른 결과를 만든다.
계약 기록은 피해자를 보호할 수 있다.
그러나 권한 없이 공개된 계약 기록은 개인의 재산 상황과 사생활을 노출할 수 있다.
대화 기록은 폭력과 협박의 증거가 될 수 있다.
그러나 맥락 없이 공개된 대화 기록은 사람을 공격하는 도구가 될 수 있다.
접속 기록은 보안 위협을 탐지할 수 있다.
그러나 과도한 접속 기록은 감시의 기반이 될 수 있다.
AI가 분석한 기록은 위험을 조기에 발견할 수 있다.
그러나 AI가 과도하게 해석한 기록은 편향된 판단이나 잘못된 추론을 만들 수 있다.
따라서 기록을 무조건 선한 것으로 볼 수 없다.
동시에 기록을 무조건 위험한 것으로만 볼 수도 없다.
기록의 본질은 중립적이다.
문제는 기록 자체가 아니라, 기록을 다루는 구조에 있다.
기록은 신뢰가 될 수도 있고 위험이 될 수도 있다.
그 차이는 기록의 존재가 아니라, 기록을 다루는 권한, 목적, 해석, 보호 구조에서 발생한다.
2.2 기록은 문명의 기억이자 권력이다
기록은 문명의 기억이다.
기록이 있기 때문에 사회는 과거의 행위를 확인할 수 있다. 계약을 기억하고, 거래를 기억하고, 승인과 거절을 기억하고, 책임과 약속을 기억한다.
기록이 없다면 문명은 많은 것을 말과 기억에 의존해야 한다.
그러나 말은 사라지고, 기억은 왜곡될 수 있다. 기록은 사라지는 행위를 붙잡아 사회적 판단의 근거로 만든다.
그러나 기록은 동시에 권력이다.
기록을 가진 사람은 해석할 수 있다.
기록에 접근할 수 있는 사람은 판단할 수 있다.
기록을 통제하는 사람은 다른 사람의 행위와 상태를 평가할 수 있다.
인공지능 시대에는 기록의 권력이 더욱 커진다.
많은 기록을 가진 주체는 AI를 통해 그 기록을 분석하고, 예측하고, 분류하고, 판단값으로 변환할 수 있다.
따라서 기록은 단순한 정보가 아니다.
기록은 사람과 조직, 사회의 관계를 바꾸는 힘이다.

기록이 공정하게 다루어지면 신뢰가 된다.
기록이 불공정하게 다루어지면 통제가 된다.
이 점에서 기록은 문명의 기억이면서 동시에 권력의 형태이다.
기록의 권력이 커질수록 중요한 것은 기록의 소유가 아니다.
중요한 것은 기록을 어떻게 다루고, 누구를 위해 쓰며, 어떤 한계 안에서 검증할 것인가이다.
2.3 기록은 악을 막을 수 있지만, 악을 조직하는 도구가 될 수도 있다
기록은 악을 막을 수 있다.
기록이 남으면 사기를 추적할 수 있고, 조작을 밝혀낼 수 있으며, 책임 회피를 줄일 수 있다. 기록은 피해자에게 증거를 제공하고, 사회가 가해자에게 책임을 물을 수 있게 한다.
기록은 부정행위를 억제한다.
기록이 남는다는 사실만으로도 사람은 함부로 거짓말하거나 조작하기 어려워진다.
그러나 기록은 악을 조직하는 도구가 될 수도 있다.
악의적인 주체는 기록을 모아 타인의 약점을 찾을 수 있다.
개인의 위치, 습관, 재산, 관계, 감정, 취약점을 파악해 협박이나 사기, 조작에 활용할 수 있다.
AI는 이 위험을 더 정교하게 만들 수 있다.
AI는 기록을 분석해 개인의 취약점을 추론하고, 특정 사람에게 맞춘 사기 메시지나 조작된 설득을 생성할 수 있다. 또한 실제처럼 보이는 허위 문서, 이미지, 음성, 영상, 대화 기록을 만들어낼 수 있다.
기록은 범죄를 막는 증거가 될 수 있지만, 범죄를 설계하는 자료가 될 수도 있다.
기록은 진실을 밝히는 도구가 될 수 있지만, 편집과 왜곡을 통해 거짓을 조직하는 도구가 될 수도 있다.
따라서 기록 사회에서 중요한 것은 단순히 기록을 늘리는 일이 아니다.
중요한 것은 기록이 악을 막는 방향으로 사용되도록 하고, 악을 조직하는 도구가 되지 않도록 권한과 보호 구조를 설계하는 일이다.
기록은 방패가 될 수 있다.
그러나 통제되지 않으면 칼이 된다.
2.4 좋은 문명은 많이 기록하는 문명이 아니라 필요한 기록을 안전하게 다루는 문명이다
좋은 문명은 많이 기록하는 문명이 아니다.

많이 기록한다고 해서 반드시 더 안전해지는 것은 아니다.
오히려 과도한 기록은 유출 위험을 키우고, 감시의 가능성을 높이며, 개인의 회복 가능성을 줄일 수 있다.
좋은 문명은 필요한 기록을 남긴다.
그리고 그 기록을 안전하게 다룬다.
필요한 기록은 책임을 만든다.
필요한 기록은 피해자를 보호한다.
필요한 기록은 사기와 조작을 줄인다.
필요한 기록은 사회적 신뢰를 만든다.
그러나 불필요한 기록, 과도한 기록, 권한 없는 기록, 목적 없는 기록은 위험이 된다.
따라서 미래 문명은 기록의 양보다 기록의 구조를 보아야 한다.
얼마나 많이 저장했는가보다, 무엇을 왜 저장했는가를 보아야 한다.
누가 접근할 수 있는가, 언제 검증할 수 있는가, 원본 정보는 어떻게 보호되는가를 보아야 한다.
좋은 문명은 모든 것을 기억하는 문명이 아니다.
좋은 문명은 기억해야 할 것을 안전하게 기억하고, 보호해야 할 것을 보호하는 문명이다.
인공지능 시대에는 이 기준이 더욱 중요해진다.
AI가 모든 기록을 분석할 수 있다고 해서 모든 기록을 AI에게 맡겨도 되는 것은 아니다. 더 강한 해석 능력은 더 강한 보호 원칙을 필요로 한다.
좋은 문명은 많이 기록하는 문명이 아니라, 필요한 기록을 안전하게 다루고, 필요한 사실만 검증하며, 인간이 스스로를 보호할 수 있도록 돕는 문명이다.
2.5 미래 신뢰 기술의 핵심은 무한 저장이 아니라 안전한 검증 구조다
미래 신뢰 기술의 핵심은 무한 저장이 아니다.
모든 정보를 저장하는 기술은 강력해 보일 수 있다.
그러나 모든 것을 저장하는 시스템은 모든 것이 유출될 수 있는 시스템이기도 하다.
진정한 신뢰 기술은 모든 정보를 들고 있는 기술이 아니다.
진정한 신뢰 기술은 필요한 사실을 필요한 순간에 안전하게 검증할 수 있는 기술이다.
사용자의 모든 정보를 공개하지 않고도, 필요한 사실을 확인할 수 있어야 한다.
계약서 전체를 저장하지 않고도, 위험 신호를 판단할 수 있어야 한다.

개인의 모든 행위를 노출하지 않고도, 특정 행위의 진위를 증명할 수 있어야 한다.
AI가 기록을 분석하더라도, 민감한 원본 정보는 보호되어야 한다.
AI가 판단값을 제공하더라도, 그 판단의 근거와 한계는 설명되어야 한다.
AI가 생성한 기록과 인간이 남긴 기록은 구분될 수 있어야 한다.
이것이 안전한 검증 구조의 방향이다.
안전한 검증 구조는 다음의 원칙을 따른다.
필요한 정보만 다룬다.
민감한 원본은 보호한다.
권한 없는 접근을 제한한다.
원본 공개보다 판단값 제공을 우선한다.
필요한 순간에만 검증 가능하게 한다.
기록의 목적과 사용 범위를 제한한다.
AI 판단은 확정이 아니라 보조 신호로 제공한다.
미래의 신뢰는 데이터의 양에서 나오지 않는다.
미래의 신뢰는 데이터를 다루는 구조에서 나온다.
따라서 미래 신뢰 기술은 더 많이 기록하는 기술이 아니라, 필요한 기록을 안전하게 증명하는 기술이어야 한다.

3. 핵심 개념 정의

3.1 기록의 정의
기록이란 인간의 행위, 상태, 선택, 관계, 거래, 인증, 판단, 승인, 거절, 접속, 창작 등이 일정한 형태로 남겨진 흔적을 의미한다.
본 문서에서 말하는 기록은 종이 문서나 공식 문서에 한정되지 않는다. 기록은 문서, 텍스트, 대화, 이미지, 음성, 영상, 접속 로그, 전자서명, 인증 내역, 위치 정보, 메타데이터, 시스템 출력값, AI 생성물, 판단 결과 등 인간의 행위와 상태가 남긴 다양한 형태의 디지털·비디지털 흔적을 포함한다.
기록은 단순히 과거를 저장하는 행위가 아니다.
기록은 과거의 행위를 현재와 미래의 판단 근거로 바꾸는 구조이다.
기록이 존재하면 사람은 기억이 아니라 근거를 통해 판단할 수 있다.
기록이 존재하면 말은 사라져도 행위의 흔적은 남는다.
인공지능 시대에는 기록의 의미가 더욱 확장된다.
기록은 단순히 보관되는 자료가 아니라, AI에 의해 분석되고, 요약되고, 분류

되고, 추론되고, 판단값으로 변환될 수 있는 신호가 된다. 동시에 AI에 의해 실제처럼 생성되거나 재구성될 수 있는 대상이 되기도 한다.
따라서 AI 시대의 기록은 단순한 보관물이 아니라, 해석·검증·판단·생성의 대상이다.
그러나 기록은 언제나 중립적으로 작동하지 않는다.
기록은 어떤 목적, 권한, 맥락, 통제 구조 안에서 다루어지는가에 따라 신뢰의 근거가 될 수도 있고, 위험의 근거가 될 수도 있다.
따라서 본 문서에서 기록은 단순 저장물이 아니라, 신뢰와 위험을 동시에 만들어낼 수 있는 문명적 흔적으로 정의한다.

3.2 신뢰 기록의 정의

신뢰 기록이란 사회적 관계, 계약, 거래, 인증, 판단, 책임을 확인하고 보호하기 위해 사용되는 기록을 의미한다.
신뢰 기록은 행위의 진위를 확인하고, 분쟁을 줄이며, 책임 소재를 명확히 하는 역할을 한다. 계약서, 거래 내역, 입금 기록, 전자서명, 인증 기록, 승인 기록, 접속 기록, 위험 확인 내역, 사용자 동의 기록 등이 이에 해당할 수 있다.
신뢰 기록의 목적은 사람을 감시하는 것이 아니다.
신뢰 기록의 목적은 약속과 책임을 확인하고, 억울함을 줄이며, 사기와 조작을 방지하는 데 있다.
예를 들어 계약에서 신뢰 기록은 “누가 어떤 조건에 동의했는가”를 확인하게 한다. 거래에서 신뢰 기록은 “돈이 언제 누구에게 이동했는가”를 확인하게 한다. 디지털 인증에서 신뢰 기록은 “해당 행위가 실제 사용자나 권한 있는 주체에 의해 이루어졌는가”를 판단하게 한다.
AI 기반 시스템에서 신뢰 기록은 위험 신호를 분석하고 이상 패턴을 발견하는 데 사용될 수 있다. 그러나 이 경우에도 신뢰 기록은 목적과 권한 안에서만 활용되어야 하며, 개인을 과도하게 분석하거나 감시하는 방식으로 사용되어서는 안 된다.
이처럼 신뢰 기록은 사회가 말이 아니라 근거를 통해 신뢰를 형성하도록 돕는다.
다만 신뢰 기록도 보호 구조 없이 과도하게 수집되거나 공개되면 위험 기록으로 변할 수 있다. 따라서 신뢰 기록은 반드시 최소 수집, 최소 저장, 권한 통제, 목적 제한의 원칙 위에서 다루어져야 한다.

3.3 위험 기록의 정의

위험 기록이란 권한 없이 수집되거나 공개될 경우 개인, 조직, 사회에 피해를 줄 수 있는 기록을 의미한다.

위험 기록은 그 내용 자체가 민감하거나, 특정 맥락에서 공개될 경우 해석과 악용의 위험이 큰 기록이다. 개인의 사생활, 정확한 주소, 금융 정보, 의료 정보, 계약서 원본, 신분 정보, 사적 대화, 내부 문서, 위치 기록, 약점이 될 수 있는 행동 기록 등이 이에 해당할 수 있다.
위험 기록은 반드시 불법적인 기록만을 의미하지 않는다.
합법적으로 생성된 기록이라도, 보호되지 않거나 권한 없는 사람에게 공개되면 위험 기록이 될 수 있다.
예를 들어 계약서는 분쟁 해결을 위한 신뢰 기록이 될 수 있다. 그러나 그 계약서가 권한 없이 공개되어 개인의 재산 상태나 주소, 관계 정보가 드러나면 위험 기록이 된다.
대화 기록은 폭력이나 협박의 증거가 될 수 있다. 그러나 맥락 없이 편집되어 공개되면 사람을 공격하는 위험 기록이 될 수 있다.
AI 시대에는 위험 기록의 범위가 더 넓어진다.
하나의 기록만으로는 민감하지 않아 보이는 정보도, 여러 기록이 결합되고 AI가 분석하면 개인의 성향, 취약점, 경제 상태, 심리 상태, 관계 구조를 추론하는 근거가 될 수 있다.
따라서 위험 기록은 기록의 형태만으로 결정되지 않는다.
위험 기록은 기록의 내용, 접근 권한, 공개 범위, 사용 목적, 해석 맥락, AI 분석 가능성에 따라 결정된다.
본 문서에서 위험 기록은 보호 구조를 잃은 기록, 또는 권한과 목적을 벗어나 인간을 해칠 수 있는 기록으로 정의한다.
3.4 권한 없는 기록의 정의
권한 없는 기록이란 당사자의 동의, 법적 근거, 정당한 목적, 접근 권한 없이 수집·저장·열람·공개·활용되는 기록을 의미한다.
기록은 권한을 가질 때 신뢰가 될 수 있다.
그러나 권한을 잃으면 폭력이 될 수 있다.
권한 없는 기록은 여러 방식으로 발생한다. 동의 없이 대화를 녹음하거나, 목적 없이 개인정보를 수집하거나, 필요 이상의 데이터를 저장하거나, 내부 자료를 무단으로 외부에 공개하거나, 시스템 접근 권한을 넘어서 타인의 기록을 열람하는 경우가 이에 해당한다.
권한 없는 기록은 단순한 정보 유출 문제가 아니다.
그것은 인간의 자기결정권, 사생활, 안전, 평판, 경제적 안정, 사회적 관계를 위협할 수 있다.
기록은 어떤 사람의 삶을 설명할 수 있는 힘을 가진다.

그 기록을 권한 없이 소유하거나 해석하거나 공개하는 것은, 그 사람의 삶에 대한 통제력을 빼앗는 행위가 될 수 있다.
AI가 권한 없는 기록을 분석할 경우 위험은 더 커질 수 있다. 단순히 기록이 공개되는 것을 넘어, 공개된 기록을 바탕으로 개인의 취약성이나 행동 패턴이 추론될 수 있기 때문이다.
따라서 본 문서에서 권한 없는 기록은 신뢰를 위한 기록이 아니라 인간을 통제하거나 해칠 수 있는 비정당한 기록 상태로 정의한다.
기록의 윤리성은 기록의 존재 여부만으로 결정되지 않는다.
그 기록에 접근할 권한이 있는가, 그 목적이 정당한가, 그 범위가 필요한 만큼 제한되어 있는가가 함께 판단되어야 한다.
3.5 선택적 공개의 정의
선택적 공개란 원본 정보 전체를 공개하지 않고, 필요한 사실이나 상태만 제한적으로 증명하거나 제공하는 방식을 의미한다.
선택적 공개는 신뢰와 사생활 보호를 동시에 달성하기 위한 핵심 원칙이다. 모든 정보를 공개해야만 신뢰가 생기는 것은 아니다. 오히려 신뢰에 필요한 최소한의 사실만 공개하는 것이 더 안전할 수 있다.
예를 들어 어떤 사람이 성인인지 확인해야 할 때, 주민등록번호 전체나 주소 전체를 공개할 필요는 없다. “성인 여부”만 확인되면 충분하다.
부동산 계약에서도 마찬가지다. 계약 전 위험 판단에 필요한 것은 사용자의 모든 사생활이 아니다. 필요한 것은 소유자 일치 여부, 근저당 확인 여부, 보증보험 가능 여부, 계약 압박 신호, 설명 불일치 여부와 같은 위험 신호다.
선택적 공개는 원본의 무분별한 노출을 줄인다.
선택적 공개는 필요한 검증은 가능하게 하되, 불필요한 사생활 침해는 줄인다.
AI 기반 신뢰 기술에서도 선택적 공개는 중요하다. AI가 판단을 보조하기 위해 모든 원본 기록을 저장하거나 열람할 필요는 없다. 필요한 신호만 제공하고, 민감한 원본은 보호하는 구조가 더 안전하다.
본 문서에서 선택적 공개는 원본 정보의 전체 공개를 피하고, 신뢰 판단에 필요한 최소 사실만 제공하는 보호형 검증 방식으로 정의한다.
선택적 공개는 기록 사회에서 매우 중요한 원칙이다.
미래 신뢰 기술은 더 많은 정보를 보여주는 기술이 아니라, 필요한 정보만 안전하게 보여주는 기술이어야 한다.
3.6 최소 수집의 정의
최소 수집이란 서비스, 시스템, 기관, 플랫폼이 목적 달성에 필요한 최소한의 정보만 수집해야 한다는 원칙을 의미한다.

기록 사회에서 많은 시스템은 더 많은 데이터를 수집하려는 방향으로 움직인다. 더 많은 데이터는 더 정교한 분석을 가능하게 할 수 있다. 그러나 동시에 더 많은 데이터는 더 큰 유출 위험, 더 큰 감시 가능성, 더 큰 오남용 가능성을 만든다.
따라서 신뢰 기술은 “수집할 수 있는 모든 것”을 수집해서는 안 된다.
수집해야 하는 것은 “목적 달성에 필요한 것”이어야 한다.
예를 들어 계약 전 위험 판단을 위해 반드시 필요한 것은 사용자의 모든 개인정보가 아니다. 정확한 신분 정보나 계약서 원본 전체 없이도, 사용자가 확인한 위험 신호와 조건만으로 1차적인 판단 보조가 가능할 수 있다.
AI 기반 분석에서도 최소 수집은 중요하다.
AI가 더 많은 데이터를 입력받을수록 더 좋은 판단을 한다고 단정할 수 없다. 오히려 불필요한 민감 정보가 포함되면 유출 위험, 편향 위험, 과도한 추론 위험이 커질 수 있다.
최소 수집은 기술의 약함이 아니다.
오히려 최소 수집은 안전한 기술 설계의 출발점이다.
본 문서에서 최소 수집은 신뢰 판단에 필요한 범위를 넘어서 데이터를 수집하지 않는 원칙으로 정의한다.
최소 수집은 인간을 보호하기 위한 기술적 겸손이다.
모든 것을 알 수 있다고 해서 모든 것을 가져도 되는 것은 아니다.
3.7 최소 저장의 정의
최소 저장이란 수집된 정보라 하더라도 목적 달성에 필요하지 않거나, 장기 보관의 정당성이 부족한 정보는 저장하지 않거나, 가능한 한 짧게 보관하고, 익명화·비식별화·삭제·만료 처리해야 한다는 원칙을 의미한다.
최소 수집이 “무엇을 받을 것인가”의 문제라면, 최소 저장은 “무엇을 남길 것인가”의 문제이다.
정보는 수집되는 순간부터 위험이 된다.
저장되는 순간 그 위험은 지속된다.
오래 저장될수록 유출, 해킹, 오남용, 목적 외 사용 가능성은 커진다.
따라서 미래 신뢰 기술은 정보를 수집한 뒤 무한히 저장하는 방식으로 설계되어서는 안 된다.
필요한 순간에만 처리하고, 목적이 끝나면 남기지 않는 구조가 필요하다. 남겨야 한다면 원본이 아니라 비식별화된 통계, 판단값, 상태값, 개선에 필요한 최소 정보만 남기는 방향이 안전하다.
AI 기반 시스템에서도 최소 저장은 중요하다.

모델 개선이나 판단 고도화를 이유로 민감한 원본 기록을 계속 저장하는 것은 위험할 수 있다. 목적이 끝난 기록은 최소화되어야 하며, AI 학습이나 분석에 활용되는 정보 역시 보호 원칙을 따라야 한다.
본 문서에서 최소 저장은 신뢰 형성에 필요한 범위를 넘어서 기록을 장기 보관하지 않는 원칙으로 정의한다.
좋은 시스템은 모든 것을 오래 기억하는 시스템이 아니다.
좋은 시스템은 기억해야 할 것과 잊어야 할 것을 구분하는 시스템이다.
3.8 검증 가능한 판단값의 정의
검증 가능한 판단값이란 원본 정보를 모두 공개하지 않더라도, 특정 상태나 위험 신호, 확인 여부, 신뢰 수준을 판단할 수 있도록 구조화된 결과값을 의미한다.
판단값은 원본 정보와 다르다.
원본 정보는 상세한 사실 전체를 담고 있지만, 판단값은 그중 특정 목적에 필요한 의미를 추출해 제공한다.
예를 들어 계약서 원본 전체를 공개하지 않아도 “소유자 일치 확인 필요”, “근저당 확인 필요”, “계약 압박 신호 감지”, “추가 상담 권고”와 같은 판단값을 제공할 수 있다.
Trust Score도 판단값의 한 형태가 될 수 있다.
PASS/HOLD/STOP도 판단값의 한 형태가 될 수 있다.
검증 가능한 판단값은 사용자에게 두 가지 이점을 제공한다.
첫째, 원본 정보 전체를 노출하지 않고도 중요한 의미를 이해하게 한다.
둘째, 사용자가 다음 행동을 선택할 수 있도록 돕는다.
AI는 판단값을 생성하거나 보조하는 데 활용될 수 있다. 그러나 AI가 제공한 판단값은 반드시 근거와 한계를 함께 가져야 한다. AI 판단값은 확정적 진실이 아니라, 입력된 기록과 신호를 바탕으로 한 판단 보조 결과여야 한다.
따라서 판단값은 절대적 확정이 아니다.
판단값은 위험 신호를 구조화한 결과이며, 사용자의 추가 확인과 전문가 상담을 대체하지 않는다.
본 문서에서 검증 가능한 판단값은 원본의 무분별한 공개를 줄이면서도 사용자가 위험과 신뢰 상태를 이해할 수 있도록 제공되는 구조화된 결과로 정의한다.
3.9 신뢰 기록 최소화 원칙의 정의
신뢰 기록 최소화 원칙이란 신뢰 형성을 위해 모든 정보를 수집하고 저장하는 것이 아니라, 필요한 기록만 최소한으로 수집·구조화하고, 민감한 원본 정보는

보호하며, 필요한 순간에만 검증 가능한 판단값을 제공해야 한다는 원칙이다.
이 원칙은 기록의 양보다 기록의 구조를 중시한다.
더 많이 저장하는 것이 더 높은 신뢰를 의미하지 않는다. 신뢰는 필요한 정보를 안전하게 다루는 구조에서 나온다.
신뢰 기록 최소화 원칙은 다음의 방향을 가진다.
필요한 정보만 수집한다.
목적이 끝난 정보는 저장하지 않는다.
민감한 원본 정보는 보호한다.
원본 공개보다 판단값 제공을 우선한다.
권한 있는 주체만 접근하게 한다.
필요한 순간에만 검증 가능하게 한다.
사용자의 통제권을 보장한다.
AI 판단은 설명 가능하고 한계를 가져야 한다.
이 원칙은 특히 디지털 계약, 신원 인증, 전자서명, AI 분석, 위험 판단, 디지털 실존 증명과 같은 영역에서 중요하다.
본 문서에서 신뢰 기록 최소화 원칙은 기록을 통해 신뢰를 만들되, 기록이 인간을 해치지 않도록 제한하고 보호하는 미래 신뢰 기술의 기본 원칙으로 정의한다.
3.10 기록의 양면성 원리의 정의
기록의 양면성 원리란 기록이 신뢰와 보호의 도구가 될 수 있는 동시에, 감시와 협박, 조작과 범죄 모의의 도구가 될 수도 있다는 관점이다.
기록은 문명의 방패가 될 수 있다.
기록은 계약을 증명하고, 거래를 추적하며, 책임을 묻고, 피해자를 보호할 수 있다.
그러나 기록은 문명의 칼이 될 수도 있다.
기록은 사생활을 노출하고, 약점을 수집하며, 권력의 감시를 가능하게 하고, 범죄자가 더 정교한 악을 모의하는 자료가 될 수 있다.
인공지능 시대에는 이 양면성이 더욱 강해진다.
AI는 기록을 분석해 위험을 조기에 발견할 수 있지만, 동시에 기록을 과도하게 추론하고, 조작된 기록을 생성하며, 개인을 예측과 통제의 대상으로 만들 수도 있다.
따라서 기록은 그 자체로 선하거나 악한 것이 아니다.
기록은 권한, 목적, 공개 범위, 통제 구조, 보호 수준, 해석 방식에 따라 신뢰가 되기도 하고 위험이 되기도 한다.

본 문서에서 기록의 양면성 원리는 다음과 같이 정의한다.
기록은 신뢰를 만드는 문명의 기억이지만, 통제되지 않으면 인간을 해칠 수 있는 위험의 구조가 된다. 따라서 미래 신뢰 기술은 더 많이 기록하는 기술이 아니라, 필요한 기록만 안전하게 구조화하고 필요한 순간에만 검증 가능하게 하는 기술이어야 한다.

4. 기록의 양면성 구조

기록은 신뢰를 만드는 기반이 될 수 있지만, 동시에 위험을 만드는 기반이 될 수도 있다.
같은 기록이라도 어떤 목적과 권한, 맥락, 보호 구조 안에서 사용되는가에 따라 전혀 다른 결과를 만든다. 계약서는 피해자를 보호하는 증거가 될 수 있지만, 권한 없이 공개되면 사생활과 재산 정보를 노출하는 위험 기록이 될 수 있다. 대화 기록은 폭력과 협박의 증거가 될 수 있지만, 일부만 잘려 공개되면 사람을 공격하는 도구가 될 수 있다.
따라서 기록은 단순한 데이터가 아니다.
기록은 신뢰와 위험이 동시에 분화될 수 있는 문명적 구조다.
본 장에서는 기록이 어떤 방식으로 긍정적 기능과 부정적 기능을 동시에 갖는지, 기록이 어떻게 방패가 되고 칼이 되는지, 그리고 기록이 어떻게 진실을 밝히거나 조작된 진실을 만들 수 있는지를 정리한다.
4.1 기록의 긍정적 기능
기록은 사회적 신뢰를 형성하는 긍정적 기능을 가진다.
기록은 행위의 흔적을 남기고, 그 흔적을 바탕으로 책임을 확인하게 한다. 계약에서 기록은 약속의 내용을 보존하고, 거래에서 기록은 돈의 흐름을 확인하게 하며, 인증에서 기록은 권한 있는 주체의 행위를 증명하게 한다.
기록은 사기와 조작을 줄일 수 있다.
행위가 기록된다는 사실은 부정행위를 억제하고, 문제가 발생했을 때 원인을 추적할 수 있게 한다.
기록은 피해자를 보호할 수 있다.
기록이 없다면 피해자는 말로만 자신의 상황을 설명해야 한다. 그러나 기록이 있다면 피해자는 사실에 기반해 억울함을 증명할 수 있다.
기록은 사회적 책임을 강화한다.
권한을 가진 사람, 기관, 플랫폼, 기업, 공공 시스템은 기록을 통해 자신들의 행위에 대해 설명해야 한다.

이 점에서 기록은 투명성, 책임성, 검증 가능성, 신뢰를 만드는 문명의 기반이다.
인공지능 시대에는 기록의 긍정적 기능이 더 확장될 수 있다.
AI는 많은 기록 속에서 사람이 놓치기 쉬운 위험 신호를 발견하고, 복잡한 문서를 요약하며, 이상 거래나 비정상 접근을 탐지할 수 있다. 이러한 기능은 사기 예방, 계약 위험 점검, 보이스피싱 탐지, 출처 검증, 디지털 실존 확인에 도움을 줄 수 있다.
기록은 사라지는 행위를 붙잡아 사회적 판단의 근거로 만든다.
따라서 기록은 인간 사회가 기억과 말에만 의존하지 않고, 근거와 책임 위에서 작동하도록 돕는다.
4.2 기록의 부정적 기능
기록은 부정적 기능도 가진다.
기록은 한 사람의 삶을 보호할 수 있지만, 동시에 한 사람의 삶을 노출시킬 수 있다. 사생활, 감정, 관계, 금융 상태, 건강 정보, 위치, 대화, 실수, 약점이 기록되고 공개되면, 그 기록은 개인을 공격하는 도구가 된다.
기록은 감시를 가능하게 한다.
모든 행위가 기록되고 분석되는 사회에서는 개인이 자유롭게 행동하기 어려워질 수 있다. 사람은 항상 평가받고 감시받는다고 느끼며, 자기검열을 하게 된다.
기록은 조작될 수 있다.
기록은 사실을 담을 수 있지만, 기록의 일부만 선택되거나 맥락이 제거되면 사실과 다른 의미를 만들어낼 수 있다.
기록은 범죄에 악용될 수 있다.
누군가의 습관, 위치, 자산, 관계, 취약점이 기록으로 남으면, 악의적인 주체는 그 기록을 이용해 더 정교한 사기와 협박을 설계할 수 있다.
인공지능은 이러한 부정적 기능을 증폭시킬 수 있다.
AI는 흩어진 기록을 결합해 사용자가 직접 공개하지 않은 민감한 사실을 추론할 수 있고, 특정 개인의 취약점에 맞춘 조작된 메시지나 허위 기록을 생성할 수 있다.
따라서 기록은 무조건 많이 남긴다고 좋은 것이 아니다.
기록의 부정적 기능은 기록 자체에서만 오는 것이 아니라, 기록을 다루는 권한과 보호 구조의 부재에서 발생한다.
보호되지 않은 기록은 신뢰가 아니라 위험이 된다.
4.3 기록이 방패가 되는 경우

기록은 방패가 될 수 있다.
기록이 방패가 되는 경우는 기록이 사람을 보호하고, 위험을 줄이며, 책임을 분명히 할 때이다.
계약 기록은 계약 당사자를 보호한다.
계약서와 특약 사항이 남아 있으면, 나중에 분쟁이 발생했을 때 각자가 어떤 조건에 동의했는지 확인할 수 있다.
거래 기록은 돈의 흐름을 보호한다.
입금과 송금 내역은 누가 언제 얼마를 지급했는지 확인하게 한다.
인증 기록은 권한을 보호한다.
누가 어떤 시스템에 접근했고, 어떤 행위를 승인했는지 확인할 수 있다.
대화 기록은 피해자를 보호할 수 있다.
협박, 폭력, 사기, 강요의 정황이 기록되어 있다면, 피해자는 자신의 상황을 입증할 수 있다.
위험 확인 기록은 사용자를 보호할 수 있다.
부동산 계약 전 어떤 위험 신호를 확인했는지, 어떤 항목이 불확실했는지, 어떤 추가 확인이 필요했는지를 기록하거나 판단값으로 남기면 사용자는 더 신중한 결정을 내릴 수 있다.
AI 기반 분석 역시 방패가 될 수 있다.
AI는 계약서의 위험 문구를 찾아내고, 보이스피싱 가능성이 높은 대화 패턴을 감지하며, 허위 생성물과 조작된 기록을 탐지하는 데 도움을 줄 수 있다.
이처럼 기록은 약속을 보호하고, 책임을 남기며, 억울함을 줄이는 방패가 된다.
다만 기록이 방패가 되기 위해서는 권한과 목적이 분명해야 한다.
방패가 되기 위해 만든 기록도 보호 구조가 없으면 칼이 될 수 있다.
4.4 기록이 칼이 되는 경우
기록은 칼이 될 수 있다.
기록이 칼이 되는 경우는 기록이 사람을 보호하는 것이 아니라 공격하고, 통제하고, 협박하고, 조작하는 데 사용될 때이다.
권한 없이 공개된 사생활 기록은 개인을 공격하는 칼이 된다.
개인의 대화, 사진, 위치, 감정, 건강 정보, 경제 상태가 공개되면 그 기록은 회복하기 어려운 피해를 만들 수 있다.
맥락 없이 편집된 기록은 평판을 공격하는 칼이 된다.
전체 맥락을 제거한 일부 기록은 사람을 오해하게 만들고, 사실과 다른 판단을 유도할 수 있다.

감시 목적의 기록은 자유를 억압하는 칼이 된다.
모든 행위가 기록되고 평가된다는 감각은 인간을 위축시키고, 스스로를 검열하게 만든다.
범죄자가 수집한 기록은 범죄의 칼이 된다.
위치 기록, 습관, 자산 정보, 가족 관계, 심리적 취약점은 사기, 협박, 스토킹, 범죄 모의에 악용될 수 있다.
AI가 결합되면 기록의 칼은 더 날카로워질 수 있다.
AI는 개인의 약점을 분석하고, 맞춤형 사기 문구를 만들고, 실제처럼 보이는 허위 이미지·음성·문서·대화 기록을 생성할 수 있다.
따라서 기록은 반드시 보호되어야 한다.
기록이 칼이 되는 순간, 기록은 더 이상 신뢰의 기반이 아니라 위험의 기반이 된다.
기록을 남기는 사회는 동시에 기록을 보호하는 사회여야 한다.
보호 없는 기록은 문명의 발전이 아니라 문명의 취약점이 된다.
4.5 기록이 증거가 되는 경우
기록은 증거가 될 수 있다.
기록이 증거가 되는 경우는 과거의 행위, 약속, 승인, 거래, 책임, 위험 신호를 확인할 수 있을 때이다.
계약서가 있으면 계약 조건을 확인할 수 있다.
입금 내역이 있으면 금전 이동을 확인할 수 있다.
전자서명이 있으면 동의와 승인의 흔적을 확인할 수 있다.
접속 기록이 있으면 시스템 접근과 행위 시점을 확인할 수 있다.
상담 기록이나 확인 기록이 있으면 어떤 설명과 안내가 이루어졌는지 확인할 수 있다.
기록이 증거가 되려면 몇 가지 조건이 필요하다.
첫째, 기록의 시점이 확인되어야 한다.
둘째, 기록의 주체가 확인되어야 한다.
셋째, 기록의 내용이 조작되지 않았다는 신뢰가 있어야 한다.
넷째, 기록이 생성된 맥락을 함께 고려해야 한다.
다섯째, 기록에 접근하고 사용하는 권한이 정당해야 한다.
AI 시대에는 여기에 한 가지 조건이 더 추가된다.
그 기록이 인간의 실제 행위에서 나온 것인지, AI에 의해 생성되거나 조작된 것인지 검증할 수 있어야 한다.
증거로서의 기록은 사회적 신뢰를 강화한다.

기록이 없다면 판단은 주장과 기억에 의존하게 된다.
기록이 있으면 판단은 근거와 책임에 가까워진다.
그러나 기록이 증거가 된다는 이유만으로 모든 기록을 무제한 수집하고 저장해서는 안 된다.
증거의 필요성과 사생활 보호는 함께 설계되어야 한다.
4.6 기록이 협박과 감시의 도구가 되는 경우
기록은 협박과 감시의 도구가 될 수 있다.
기록이 협박의 도구가 되는 경우는 기록이 개인의 약점, 사생활, 비밀, 실수, 관계, 경제 상태를 노출시킬 수 있을 때이다.
악의적인 주체는 기록을 이용해 상대를 압박할 수 있다.
“이 기록을 공개하겠다”는 위협은 기록을 단순한 정보가 아니라 폭력의 수단으로 만든다.
기록이 감시의 도구가 되는 경우는 개인의 행동이 지속적으로 추적되고 분석될 때이다.
위치, 접속, 소비, 대화, 검색, 관계, 이동, 판단이 모두 기록되고 연결되면, 개인은 자기 삶을 스스로 선택하는 존재가 아니라 관찰되는 대상이 될 수 있다.
감시는 항상 강제적으로만 작동하지 않는다.
사람은 자신이 기록되고 있다는 사실만으로도 행동을 조심하고, 말과 감정을 숨기며, 스스로를 검열하게 된다.
기록을 통한 감시는 눈에 보이지 않는 통제가 될 수 있다.
인공지능이 감시 구조와 결합될 경우 이 위험은 더 커진다.
AI는 수많은 기록을 빠르게 분석하고, 사람의 행동 패턴을 예측하며, 개인의 취약한 지점을 찾아낼 수 있다. 이러한 기술이 보호가 아니라 통제의 목적으로 사용될 경우, 기록은 감시의 기반이 된다.
따라서 기록이 협박과 감시의 도구가 되지 않도록 하기 위해서는 접근 권한, 보관 기간, 목적 제한, 삭제 가능성, 선택적 공개, 비식별화, 사용자 통제권이 필요하다.
기록은 사람을 보호해야 한다.
기록이 사람을 침묵하게 만들고 통제한다면, 그것은 신뢰 기술이 아니라 감시 기술이다.
4.7 기록이 진실을 밝히는 경우
기록은 진실을 밝힐 수 있다.
기억은 흐려질 수 있고, 말은 바뀔 수 있으며, 권력은 사실을 덮을 수 있다.
그러나 기록은 사라진 행위의 흔적을 남겨 진실에 접근할 수 있는 근거를 제

공한다.
기록은 누가 무엇을 했는지 밝힐 수 있다.
기록은 어떤 약속이 있었는지 확인할 수 있게 한다.
기록은 어떤 거래가 실제로 이루어졌는지 보여줄 수 있다.
기록은 어떤 위험 신호가 사전에 존재했는지 드러낼 수 있다.
사회적 약자에게 기록은 특히 중요하다.
힘의 차이가 큰 관계에서 말만으로는 진실을 입증하기 어렵다.
기록은 약자가 자신의 피해와 상황을 설명할 수 있는 근거가 된다.
기록은 부정과 은폐를 줄인다.
기록이 남아 있으면 거짓 해명과 책임 회피가 어려워진다.
AI는 진실을 밝히는 데 도움을 줄 수도 있다.
AI는 많은 문서와 로그 속에서 이상 패턴을 찾고, 시간 순서를 정리하며, 사람이 놓친 위험 신호를 발견할 수 있다.
이 점에서 기록은 진실을 향한 문명의 도구다.
그러나 기록이 진실을 밝히기 위해서는 기록의 전체 맥락과 무결성이 중요하다.
일부만 남은 기록, 편집된 기록, 조작된 기록은 오히려 진실을 왜곡할 수 있다.
따라서 기록은 진실을 밝히는 도구가 될 수 있지만, 그 기록이 어떻게 생성되고 보존되고 해석되는지도 함께 검토되어야 한다.
4.8 기록이 조작된 진실을 만드는 경우
기록은 조작된 진실을 만들 수도 있다.
사람들은 기록이 있으면 그것을 곧 사실이라고 믿기 쉽다.
그러나 기록은 언제나 전체 진실을 담고 있지 않다. 기록은 특정 시점, 특정 관점, 특정 장면, 특정 문장만을 담을 수 있다.
기록의 일부만 선택하면 전혀 다른 이야기를 만들 수 있다.
맥락을 제거하면 정당한 말도 공격적인 말처럼 보일 수 있고, 방어적 행동도 가해처럼 보일 수 있다.
편집된 영상, 잘린 대화, 일부 캡처, 왜곡된 통계, 조작된 로그는 진실처럼 보이는 거짓을 만들 수 있다.
디지털 사회에서는 이러한 위험이 더 커진다.
AI 생성물, 딥페이크, 합성 음성, 조작 이미지, 위조 문서, 편집된 기록은 기록의 신뢰성을 흔들 수 있다.
AI는 실제처럼 보이는 기록을 만들 수 있다.

존재하지 않은 음성, 촬영되지 않은 영상, 작성되지 않은 문서, 실제 대화처럼 보이는 텍스트를 생성할 수 있다. 이때 기록은 과거의 흔적이 아니라, 과거가 있었던 것처럼 보이게 만드는 조작물이 될 수 있다.
기록은 진실을 밝힐 수 있지만, 조작된 기록은 진실의 얼굴을 한 거짓이 될 수 있다.
따라서 미래 신뢰 기술은 단순히 기록을 남기는 것에 머물러서는 안 된다.
기록의 출처, 시점, 맥락, 무결성, 변경 여부, 접근 권한, AI 생성 여부를 함께 검증해야 한다.
기록이 진실이 되기 위해서는 기록의 존재만으로는 부족하다.
기록이 어떻게 만들어졌고, 어떻게 보존되었으며, 어떤 맥락에서 해석되어야 하는지를 함께 확인해야 한다.
이것이 기록 사회에서 신뢰 기술이 필요한 이유이다.

5. 기록의 위험 분류

기록은 신뢰를 만드는 기반이 될 수 있지만, 동시에 인간과 사회를 위험하게 만들 수 있다.
기록의 위험은 단순히 “정보가 유출되었다”는 문제에만 머물지 않는다. 기록은 개인의 사생활을 노출시키고, 비밀 정보를 외부에 드러내며, 감시와 통제의 기반이 되고, 협박과 조작, 범죄 모의의 도구가 될 수 있다.
인공지능의 발전은 이러한 위험을 더욱 확대한다.
AI는 기록을 단순히 저장된 정보로 두지 않고, 분석하고 추론하고 생성할 수 있다. 이로 인해 기록은 유출 위험을 넘어, 예측과 조작, 허위 생성의 위험까지 가지게 된다.
따라서 기록 사회에서 중요한 것은 기록의 존재 여부만이 아니다.
중요한 것은 어떤 기록이 어떤 위험을 만들 수 있는지 분류하고, 그 위험을 사전에 인식하는 일이다.
본 장에서는 기록이 만들어낼 수 있는 주요 위험을 분류한다.

5.1 사생활 노출 위험

사생활 노출 위험이란 개인의 사적 정보가 권한 없이 공개되거나, 원래 목적을 벗어나 타인에게 노출됨으로써 개인의 존엄, 안전, 평판, 관계, 경제적 안정에 피해를 주는 위험을 의미한다.
디지털 사회에서 사생활은 단순히 집 안에서의 생활만을 의미하지 않는다.
대화 기록, 위치 기록, 검색 기록, 구매 기록, 금융 기록, 의료 기록, 상담 기록, 사진, 영상, 감정 표현, 인간관계, 소비 습관, 이동 경로까지 모두 사생활의 일부가 될 수 있다.

사생활 기록은 개인을 이해하는 단서가 될 수 있지만, 동시에 개인을 공격하는 재료가 될 수도 있다.
예를 들어 개인의 위치 기록이 공개되면 생활 패턴이 노출될 수 있다.
대화 기록이 공개되면 사적인 관계와 감정이 노출될 수 있다.
금융 기록이 공개되면 경제 상태와 취약점이 드러날 수 있다.
의료 기록이 공개되면 사회적 편견이나 차별의 대상이 될 수 있다.
AI가 이러한 기록을 분석하면 위험은 더 커질 수 있다.
겉으로는 평범해 보이는 기록도 여러 데이터와 결합되면 개인의 심리, 경제 상황, 취약성, 생활 습관을 추론하는 근거가 될 수 있다.
사생활 노출의 문제는 단순한 불편함이 아니다.
한번 공개된 기록은 완전히 회수하기 어렵고, 개인의 삶에 오래 남을 수 있다.
따라서 사생활 기록은 원칙적으로 최소한으로 수집되어야 하며, 수집된 경우에도 명확한 목적과 권한, 보호 구조 안에서만 다루어져야 한다.
사생활은 숨겨야 할 부끄러운 것이 아니라, 인간이 인간답게 살아가기 위해 필요한 보호 영역이다.
기록 사회에서 사생활 보호는 선택이 아니라 신뢰 기술의 기본 조건이다.
5.2 비밀 정보 유출 위험
비밀 정보 유출 위험이란 개인, 조직, 기업, 기관이 보호해야 할 내부 기록이나 민감 정보가 권한 없이 외부로 공개됨으로써 피해가 발생하는 위험을 의미한다.
비밀 정보는 개인의 사생활뿐 아니라 조직의 전략, 계약, 연구, 기술, 재무, 고객 정보, 내부 의사결정, 법률 검토 내용 등을 포함할 수 있다.
비밀 정보가 유출되면 여러 문제가 발생한다.
첫째, 개인의 안전과 권리가 침해될 수 있다.
고객 정보, 상담 기록, 계약 정보, 신원 정보가 외부에 공개되면 개인은 사기, 협박, 스토킹, 금융 피해 등의 위험에 노출될 수 있다.
둘째, 조직의 경쟁력이 훼손될 수 있다.
기술 문서, 사업 전략, 내부 검토 자료, 계약 조건이 유출되면 조직은 경쟁상 불이익을 입을 수 있다.
셋째, 사회적 신뢰가 붕괴될 수 있다.
기관이나 기업이 보관하던 기록이 유출되면 사람들은 더 이상 그 시스템을 신뢰하지 못하게 된다.
넷째, 기록의 맥락이 왜곡될 수 있다.
비밀 정보는 내부 검토 과정의 일부일 수 있다. 그러나 외부에 일부만 공개되

면 사실과 다른 해석을 만들 수 있다.
AI 시대에는 비밀 정보 유출의 위험이 더 복잡해진다.
유출된 정보는 단순히 공개되는 데서 끝나지 않고, AI에 의해 요약되고 재구성되고 분석되어 더 큰 피해로 확장될 수 있다. 또한 AI는 유출 정보를 바탕으로 더 정교한 공격 시나리오를 생성할 수도 있다.
따라서 비밀 기록은 단순히 숨기는 것이 목적이 아니다.
보호되어야 할 기록은 명확한 권한, 접근 통제, 보관 기간, 사용 목적, 유출 대응 체계 안에서 관리되어야 한다.
비밀 정보 보호는 폐쇄성을 위한 것이 아니라, 신뢰를 유지하기 위한 조건이다.
5.3 감시와 통제 위험
감시와 통제 위험이란 기록이 개인의 행동을 지속적으로 추적하고 평가하며, 그 결과 개인의 자유와 선택을 제한하는 구조로 작동하는 위험을 의미한다.
기록은 보안을 위해 필요할 수 있다.
접속 기록, 거래 기록, 위치 기록, 인증 기록은 이상 행위를 탐지하고 책임을 확인하는 데 도움이 된다.
그러나 모든 행위가 기록되고, 그 기록이 지속적으로 분석되고, 개인이 그 사실을 알거나 통제할 수 없다면 기록은 감시의 기반이 된다.
감시는 반드시 눈에 보이는 강압으로만 작동하지 않는다.
사람은 자신이 기록되고 있다는 사실만으로도 행동을 조심한다.
말을 줄이고, 감정을 숨기고, 선택을 바꾸고, 스스로를 검열한다.
이때 기록은 자유를 보호하는 장치가 아니라 자유를 줄이는 장치가 된다.
감시와 통제 위험은 특히 권력이 한쪽에 집중될 때 커진다.
플랫폼, 기업, 기관, 국가가 개인의 기록을 과도하게 보유하고 분석할 수 있다면, 개인은 자신에 대한 판단이 어떻게 이루어지는지 알기 어렵다.
AI는 감시와 통제 위험을 더 강화할 수 있다.
AI는 많은 기록을 빠르게 분석하고, 개인의 행동을 예측하며, 위험 인물이나 취약 계층을 자동 분류할 수 있다. 이러한 기능이 보호 목적이 아니라 통제 목적으로 사용될 경우, 기록은 인간의 자유를 제한하는 장치가 된다.
따라서 기록 기반 시스템은 반드시 다음 질문을 가져야 한다.
누가 기록을 보는가.
무엇을 위해 보는가.
어느 범위까지 보는가.
사용자는 알 수 있는가.

사용자는 거부하거나 통제할 수 있는가.
기록은 언제 삭제되거나 만료되는가.
AI가 판단한다면 그 기준과 한계는 설명되는가.
기록이 신뢰가 되려면 감시가 아니라 보호를 위한 구조여야 한다.
5.4 협박과 약점 수집 위험
협박과 약점 수집 위험이란 기록이 개인이나 조직의 취약점을 파악하고, 이를 압박·협박·조작·이익 추구의 수단으로 활용하는 위험을 의미한다.
기록은 사람의 약점을 드러낼 수 있다.
경제적 어려움, 건강 문제, 인간관계, 사적 대화, 실수, 감정적 표현, 위치와 생활 패턴, 계약 관계, 채무 관계, 개인적 고민까지 기록으로 남을 수 있다.
악의적인 주체는 이러한 기록을 단순 정보로 보지 않는다.
그들은 기록을 이용해 상대를 통제할 수 있는 지점을 찾는다.
예를 들어 사적인 대화 기록은 협박의 도구가 될 수 있다.
금융 기록은 경제적 취약성을 노리는 사기의 출발점이 될 수 있다.
위치 기록은 스토킹이나 물리적 위협의 자료가 될 수 있다.
계약 기록은 법적·경제적 압박의 수단으로 악용될 수 있다.
협박은 기록의 공개 가능성을 무기로 삼는다.
“이 기록을 공개하겠다”는 말은 기록을 정보가 아니라 폭력의 도구로 만든다.
AI는 약점 수집을 더 정교하게 만들 수 있다.
AI는 공개된 기록과 유출된 정보를 분석해 개인의 심리적 취약점, 경제적 불안, 관계적 약점, 반복 행동 패턴을 찾아낼 수 있다. 이를 바탕으로 맞춤형 사기, 협박, 조작된 설득이 가능해질 수 있다.
따라서 기록 사회에서 중요한 것은 기록이 존재한다는 사실만이 아니다.
그 기록이 누구에게 노출될 수 있는지, 어떤 방식으로 악용될 수 있는지까지 고려해야 한다.
협박과 약점 수집을 막기 위해서는 최소 수집, 최소 저장, 접근 권한 제한, 암호화, 비식별화, 선택적 공개, 사용자 통제권이 필요하다.
기록은 약자를 보호해야 한다.
기록이 약자를 더 쉽게 공격하게 만든다면, 그것은 신뢰의 도구가 아니라 위험의 도구가 된다.
5.5 조작과 편집 위험
조작과 편집 위험이란 기록의 일부가 선택적으로 사용되거나, 맥락이 제거되거나, 내용이 변형되어 사실과 다른 의미를 만들어내는 위험을 의미한다.
기록은 사람들에게 강한 신뢰감을 준다.

사진이 있으면 사실처럼 보이고, 영상이 있으면 진실처럼 느껴지며, 문서가 있으면 객관적인 근거처럼 받아들여진다.
그러나 기록은 언제나 전체 진실을 담지 않는다.
기록은 특정 시점, 특정 각도, 특정 장면, 특정 문장만을 담을 수 있다.
기록의 일부만 잘라내면 전혀 다른 이야기를 만들 수 있다.
대화의 앞뒤 맥락을 제거하면 방어적인 말도 공격처럼 보일 수 있다.
영상의 일부만 편집하면 상황의 원인과 결과가 왜곡될 수 있다.
통계의 일부만 제시하면 실제와 다른 결론을 만들 수 있다.
디지털 기술의 발전은 조작 위험을 더 크게 만든다.
AI 생성물, 딥페이크, 합성 음성, 조작 이미지, 위조 문서, 변조된 로그는 기록의 신뢰성을 흔들 수 있다.
따라서 기록 사회에서 필요한 것은 단순히 기록을 남기는 일이 아니다.
기록의 출처, 생성 시점, 수정 이력, 전체 맥락, 무결성, 권한, 보관 과정을 함께 확인하는 구조가 필요하다.
기록은 진실을 밝힐 수 있다.
그러나 조작된 기록은 진실의 얼굴을 한 거짓이 될 수 있다.
기록을 신뢰하려면 기록의 존재만이 아니라 기록의 정합성을 검증해야 한다.
5.6 범죄 모의와 악용 위험
범죄 모의와 악용 위험이란 기록이 범죄를 예방하거나 추적하는 도구로 쓰이는 동시에, 범죄자가 더 정교한 범죄를 계획하는 자료로 활용될 수 있는 위험을 의미한다.
기록은 범죄를 막을 수 있다.
거래 기록은 금융 사기를 추적할 수 있고, 접속 기록은 해킹 경로를 확인할 수 있으며, 통화와 대화 기록은 협박이나 사기 정황을 밝힐 수 있다.
그러나 같은 기록이 범죄자에게 넘어가면 상황은 반대로 바뀐다.
범죄자는 기록을 통해 대상의 생활 패턴을 파악할 수 있다.
언제 집에 있는지, 어디로 이동하는지, 어떤 사람과 연락하는지, 어떤 금융 상태에 있는지, 어떤 불안을 가지고 있는지 파악할 수 있다.
이 정보는 보이스피싱, 스미싱, 투자 사기, 전세 사기, 스토킹, 협박, 신분 도용, 계정 탈취, 사회공학적 공격에 악용될 수 있다.
기록은 범죄자를 잡는 지도일 수 있지만, 범죄자가 피해자에게 접근하는 지도도 될 수 있다.
AI는 이 위험을 더 빠르고 정교하게 만든다.
AI는 기록을 분석해 범죄 대상의 취약점을 파악하고, 자연스러운 문장으로 맞

춤형 사기 메시지를 생성하며, 실제 기관이나 지인처럼 보이는 허위 대화와 음성을 만들 수 있다.
따라서 기록의 활용에는 반드시 접근 제한과 목적 제한이 필요하다.
기록이 필요한 기관이나 시스템에서만 사용되어야 하며, 불필요한 연결과 과도한 공개는 줄여야 한다.
특히 여러 기록이 결합될 때 위험은 커진다.
하나의 기록만으로는 큰 의미가 없어도, 위치·금융·대화·관계·계약 기록이 결합되면 개인의 취약점이 입체적으로 드러날 수 있다.
미래 신뢰 기술은 기록의 결합 위험까지 고려해야 한다.
안전한 기록은 단순히 저장된 기록이 아니라, 악용 가능성이 제한된 기록이다.
5.7 책임 회피와 기록 은폐 위험
책임 회피와 기록 은폐 위험이란 기록이 남아야 할 상황에서 기록이 의도적으로 남지 않거나, 불리한 기록이 삭제·은폐·왜곡됨으로써 책임 추적이 어려워지는 위험을 의미한다.
기록이 과도하게 많아지는 것도 위험하지만, 필요한 기록이 없는 것도 위험하다.
계약 과정에서 중요한 설명이 기록되지 않으면, 나중에 분쟁이 발생했을 때 누가 어떤 말을 했는지 확인하기 어렵다.
거래 과정에서 승인과 동의 기록이 남지 않으면, 책임 소재가 불명확해진다.
기관이나 기업의 의사결정 기록이 남지 않으면, 잘못된 결정에 대해 책임을 묻기 어렵다.
악의적인 주체는 기록을 남기지 않는 방식으로 책임을 피할 수 있다.
불리한 기록만 삭제하거나, 핵심 과정을 구두로 처리하거나, 공식 기록을 남기지 않는 방식으로 책임 추적을 어렵게 만들 수 있다.
이것은 기록 과잉의 반대편에 있는 위험이다.
좋은 기록 체계는 모든 것을 기록하는 체계가 아니다.
동시에 아무것도 남기지 않는 체계도 아니다.
좋은 기록 체계는 책임에 필요한 기록은 남기고, 사생활과 민감 정보는 보호하며, 불필요한 기록은 최소화하는 균형을 가져야 한다.
책임 회피와 기록 은폐를 막기 위해서는 중요한 행위의 시점, 주체, 승인, 설명, 변경 이력, 판단 근거가 적절히 남아야 한다.
기록은 사람을 감시하기 위한 것이 아니라 책임을 공정하게 확인하기 위한 것이어야 한다.
5.8 기록 과잉으로 인한 인간 자유 축소 위험

기록 과잉으로 인한 인간 자유 축소 위험이란 모든 행위가 기록되고 평가되는 사회에서 인간의 실수, 회복, 선택, 탐색, 변화의 자유가 줄어드는 위험을 의미한다.
인간은 완벽하지 않다.
사람은 실수하고, 후회하고, 배워가며, 변한다.
그러나 모든 말과 행동, 감정과 선택이 기록되고 영구적으로 남는다면, 인간은 실수할 자유를 잃게 된다. 과거의 한 장면, 한 문장, 한 선택이 계속 따라다니면 사람은 새롭게 시작하기 어려워진다.
기록 과잉 사회에서는 사람의 현재보다 과거 기록이 더 큰 힘을 가질 수 있다. 누군가는 이미 변했지만, 기록은 그 사람을 과거의 모습에 묶어둘 수 있다.
또한 모든 행동이 평가될 수 있다는 감각은 인간을 위축시킨다.
사람은 안전한 선택만 하게 되고, 새로운 시도를 줄이며, 자유롭게 말하고 생각하는 능력을 잃을 수 있다.
AI가 이 구조에 결합되면 위험은 더 커진다.
AI는 과거 기록을 분석해 사람을 분류하고 예측할 수 있다. 이때 사람은 현재의 변화 가능성보다 과거 기록에 의해 평가될 수 있다.
좋은 문명은 책임을 묻는 문명이어야 한다.
그러나 동시에 회복의 가능성을 남기는 문명이어야 한다.
모든 것을 영원히 기록하는 사회는 공정해 보일 수 있지만, 인간에게 지나치게 가혹한 사회가 될 수 있다.
따라서 기록 사회는 잊힐 권리, 삭제 가능성, 보관 기간 제한, 목적 제한, 맥락 복원, 재평가 가능성을 함께 고민해야 한다.
기록은 인간을 영원히 과거에 묶어두기 위해 존재해서는 안 된다.
기록은 인간이 더 안전하게 살아가도록 돕기 위해 존재해야 한다.
5.9 AI 기반 추론과 허위 기록 생성 위험
인공지능은 기록의 위험을 새로운 차원으로 확장시킨다.
기록은 원래 과거의 흔적이었다. 그러나 AI는 그 흔적을 분석해 보이지 않는 정보를 추론할 수 있다. 개인의 검색 기록, 소비 기록, 대화 기록, 위치 기록, 금융 기록, 접속 기록이 결합되면 AI는 사용자의 성향, 불안, 경제적 취약성, 관계 상태, 생활 패턴까지 추론할 수 있다.
이러한 추론은 긍정적으로 사용될 수 있다.
위험 거래를 탐지하고, 보이스피싱 신호를 발견하고, 계약서의 위험 조항을 찾아내고, 이상 접근을 감지하는 데 활용될 수 있다.
그러나 같은 기술은 악용될 수도 있다.

AI는 개인의 약점을 더 정교하게 찾아낼 수 있다.
AI는 사기 메시지를 더 그럴듯하게 만들 수 있다.
AI는 특정 사람에게 맞춘 조작된 설득과 협박을 생성할 수 있다.
AI는 실제처럼 보이는 허위 이미지, 음성, 영상, 문서, 대화 기록을 만들어낼 수 있다.
이때 기록의 문제는 단순 유출을 넘어선다.
기록이 분석되어 개인을 예측하고, 기록이 조작되어 거짓을 만들고, 기록처럼 보이는 허위 데이터가 생성되어 진실을 흔드는 문제가 발생한다.
따라서 AI 시대의 기록 위험은 세 가지로 나누어 볼 수 있다.
첫째, 기록 기반 추론 위험이다.
사용자가 직접 공개하지 않은 정보라도, 여러 기록의 조합을 통해 민감한 사실이 추론될 수 있다.
둘째, 개인화된 악용 위험이다.
AI가 개인의 취약점과 상황을 분석해 맞춤형 사기, 협박, 조작, 설득에 활용될 수 있다.
셋째, 허위 기록 생성 위험이다.
AI가 실제 기록처럼 보이는 가짜 음성, 영상, 문서, 이미지, 대화 내용을 생성해 진실과 거짓의 경계를 흐릴 수 있다.
이 위험을 줄이기 위해서는 AI가 사용하는 기록의 범위, 목적, 해석 기준, 판단 한계, 생성물 출처, 검증 가능성을 함께 설계해야 한다.
AI는 기록을 더 똑똑하게 다루는 기술이지만, 동시에 기록을 더 위험하게 만들 수 있는 기술이다.
따라서 AI 기반 기록 시스템은 더 많은 데이터를 수집하는 방향이 아니라, 필요한 신호만 안전하게 해석하고, 그 판단 근거와 한계를 설명하는 방향으로 설계되어야 한다.

6. 신뢰 기록 최소화 원칙

기록의 양면성은 하나의 결론으로 이어진다.
미래 신뢰 기술은 모든 것을 기록하는 방향으로 가서는 안 된다.
또한 필요한 기록마저 남기지 않는 방향으로 가서도 안 된다.
중요한 것은 균형이다.
신뢰를 위해 필요한 기록은 남겨야 한다.
그러나 인간을 해칠 수 있는 기록은 최소화해야 한다.

원본 정보는 보호되어야 하며, 필요한 경우에는 원본 전체가 아니라 판단값으로 제공되어야 한다.
이 원칙을 본 문서에서는 신뢰 기록 최소화 원칙이라 부른다.
신뢰 기록 최소화 원칙은 기록을 줄이자는 단순한 주장이 아니다.
이 원칙은 신뢰를 만들기 위해 기록을 사용하되, 기록이 인간을 해치지 않도록 기록의 범위, 목적, 권한, 보관, 공개 방식을 제한하자는 원칙이다.
인공지능 시대에는 이 원칙이 더욱 중요하다.
AI는 기록을 강력하게 해석할 수 있기 때문에, 어떤 기록을 수집하고 어떤 기록을 제공할 것인지는 더 신중하게 결정되어야 한다.
6.1 모든 것을 기록하지 않는다
신뢰 기록 최소화 원칙의 첫 번째 기준은 모든 것을 기록하지 않는다는 것이다.
기술적으로 기록할 수 있다고 해서 모든 것을 기록해야 하는 것은 아니다.
저장할 수 있다고 해서 저장해야 하는 것도 아니다.
모든 것을 기록하는 사회는 안전해 보일 수 있다.
그러나 모든 것이 기록되는 사회는 모든 것이 유출될 수 있는 사회이기도 하다.
모든 행위가 기록되면 사람은 자유롭게 말하고 행동하기 어려워진다.
모든 선택이 남으면 인간은 실수와 회복의 가능성을 잃는다.
모든 정보가 저장되면 시스템은 더 강력해지는 동시에 더 위험해진다.
AI 시대에는 모든 것을 기록하는 위험이 더 커진다.
기록은 단순히 저장되는 것이 아니라 분석되고, 추론되고, 예측되고, 재구성될 수 있기 때문이다.
따라서 기록은 목적이 있어야 한다.
목적 없는 기록, 불필요한 기록, 과도한 기록은 신뢰가 아니라 위험을 만든다.
기록하지 않는 것도 하나의 보호 기술이다.
좋은 시스템은 모든 것을 기억하는 시스템이 아니라, 무엇을 기억하지 않아야 하는지 아는 시스템이다.
6.2 필요한 정보만 수집한다
두 번째 원칙은 필요한 정보만 수집한다는 것이다.
정보 수집은 항상 목적과 연결되어야 한다.
어떤 서비스를 제공하기 위해 어떤 정보가 반드시 필요한지 먼저 판단해야 한다.
필요하지 않은 정보를 미리 수집하는 것은 미래의 위험을 만드는 일이다.

지금은 쓸모없어 보이는 정보도, 나중에 다른 정보와 결합되면 개인의 사생활과 취약점을 드러낼 수 있다.
예를 들어 계약 전 위험 판단을 위해 사용자의 모든 개인정보가 필요한 것은 아니다.
정확한 주소, 계약서 원본, 신분 정보, 임대인의 상세 정보 없이도 1차적인 위험 신호 입력과 판단 보조는 가능할 수 있다.
필요한 것은 목적에 맞는 최소 신호다.
계약 유형, 보증금 규모, 등기부 확인 여부, 소유자 일치 여부, 근저당 확인 여부, 보증보험 가능 여부, 계약 압박 신호, 설명 불일치 여부와 같은 정보는 위험 판단에 의미가 있을 수 있다.
그러나 그 이상의 민감 정보는 반드시 필요성을 검토해야 한다.
AI 기반 분석에서도 필요한 정보만 수집해야 한다.
AI가 더 많은 데이터를 입력받는다고 해서 반드시 더 신뢰할 수 있는 판단을 하는 것은 아니다. 불필요한 정보는 오히려 편향, 과잉 추론, 사생활 침해의 원인이 될 수 있다.
필요한 정보만 수집하는 것은 기능을 약하게 만드는 것이 아니다.
오히려 신뢰할 수 있는 시스템을 만드는 기초다.
6.3 민감한 원본 정보는 보호한다
세 번째 원칙은 민감한 원본 정보는 보호한다는 것이다.
원본 정보는 강력하다.
원본에는 맥락과 세부 내용이 담겨 있다. 그러나 바로 그 이유 때문에 원본 정보는 위험하다.
계약서 원본에는 주소, 이름, 금액, 조건, 서명, 관계 정보가 포함될 수 있다.
의료 기록 원본에는 질병, 치료, 심리 상태가 포함될 수 있다.
대화 기록 원본에는 감정, 관계, 갈등, 사적인 표현이 포함될 수 있다.
금융 기록 원본에는 경제 상태와 취약점이 포함될 수 있다.
이러한 원본 정보는 필요한 경우에만 제한적으로 다루어야 한다.
미래 신뢰 기술은 원본을 무분별하게 저장하는 방향보다, 원본에서 필요한 신호만 추출하고 원본 자체는 보호하는 방향으로 설계되어야 한다.
원본 정보는 가능한 한 사용자 통제 아래 있어야 한다.
원본을 저장해야 한다면 암호화, 접근 권한 제한, 보관 기간 제한, 삭제 가능성, 감사 기록이 함께 설계되어야 한다.
AI가 원본 정보를 분석할 경우 더 강한 보호 원칙이 필요하다.
AI는 원본 정보에서 사용자가 직접 말하지 않은 민감한 사실까지 추론할 수

있기 때문이다.
원본은 신뢰의 근거가 될 수 있지만, 동시에 가장 큰 유출 위험이 될 수 있다.
따라서 민감한 원본 정보는 신뢰 기술의 중심이 아니라 보호 대상이어야 한다.
6.4 목적이 끝난 기록은 최소화한다
네 번째 원칙은 목적이 끝난 기록은 최소화한다는 것이다.
기록은 목적을 위해 존재한다.
목적이 끝난 기록을 계속 보관하는 것은 새로운 위험을 만든다.
사용자 테스트를 위해 수집한 정보가 있다면, 테스트와 개선 목적이 끝난 뒤에는 삭제하거나 비식별화해야 한다.
일시적인 인증을 위해 사용한 정보가 있다면, 인증 후 장기 보관할 필요가 있는지 검토해야 한다.
계약 전 판단 보조를 위해 사용한 입력값이 있다면, 사용자가 원하지 않는 한 불필요하게 저장하지 않는 구조가 필요하다.
기록은 오래 저장될수록 위험이 커진다.
시간이 지나면 원래 목적은 희미해지고, 기록은 다른 목적으로 재사용될 가능성이 생긴다.
목적이 끝난 기록을 최소화하는 것은 개인정보 보호만을 위한 것이 아니다.
그것은 시스템 전체의 위험을 줄이는 방법이다.
AI 학습이나 분석을 이유로 목적이 끝난 기록을 계속 보관하는 것도 신중해야 한다.
한 번 수집된 기록이 다른 목적의 분석에 재사용될 때, 사용자는 자신의 정보가 어떻게 활용되는지 알기 어려워질 수 있다.
기록의 수명은 목적과 연결되어야 한다.
목적이 끝났다면 기록도 줄어들어야 한다.
좋은 기록 체계는 생성뿐 아니라 종료도 설계한다.
기록은 언제 남길 것인가뿐 아니라 언제 지울 것인가도 함께 정해야 한다.
6.5 권한 있는 주체만 접근하게 한다
다섯 번째 원칙은 권한 있는 주체만 접근하게 한다는 것이다.
기록은 접근 권한에 따라 신뢰가 되기도 하고 위험이 되기도 한다.
같은 기록이라도 정당한 권한을 가진 사람이 보면 보호와 검증의 도구가 될 수 있지만, 권한 없는 사람이 보면 침해와 악용의 도구가 될 수 있다.
권한은 단순히 관리자 권한을 의미하지 않는다.
누가 어떤 목적에서, 어느 범위까지, 어떤 기간 동안, 어떤 방식으로 접근할 수 있는지를 정하는 구조 전체를 의미한다.

기록 접근에는 최소 권한 원칙이 필요하다.
업무나 목적 수행에 필요한 범위까지만 접근할 수 있어야 한다.
민감한 기록은 더 강한 접근 통제가 필요하다.
원본 계약서, 신원 정보, 금융 정보, 의료 정보, 사적 대화 등은 특별한 보호 대상이 되어야 한다.
또한 접근 기록 자체도 관리되어야 한다.
누가 언제 어떤 기록에 접근했는지 확인할 수 있어야 하며, 부적절한 접근은 추적 가능해야 한다.
AI 시스템이 기록에 접근하는 경우에도 권한 구조는 필요하다.
AI가 어떤 기록을 읽을 수 있는지, 어떤 목적에서 분석할 수 있는지, 어떤 결과를 생성할 수 있는지 제한되어야 한다.
권한 없는 접근을 막지 못하는 기록 시스템은 신뢰 시스템이 아니다.
그것은 위험을 축적하는 시스템이다.
6.6 필요한 순간에만 검증 가능하게 한다
여섯 번째 원칙은 필요한 순간에만 검증 가능하게 한다는 것이다.
모든 정보를 항상 공개할 필요는 없다.
모든 기록을 상시 열람 가능하게 만들 필요도 없다.
신뢰에 필요한 것은 무제한 공개가 아니라 필요한 순간의 검증이다.
어떤 사람이 성인인지 확인할 때, 그 사람의 전체 신분 정보를 보여줄 필요는 없다.
어떤 계약의 위험 신호를 확인할 때, 계약서 전체와 사생활 전체를 공개할 필요는 없다.
어떤 행위의 진위를 확인할 때, 그 사람의 모든 디지털 기록을 열람할 필요는 없다.
필요한 것은 특정 사실의 검증이다.
해당 조건이 충족되었는지, 위험 신호가 있는지, 권한 있는 행위였는지, 특정 시점에 어떤 상태였는지 확인하면 된다.
이 원칙은 선택적 공개와 연결된다.
전체를 공개하지 않고도 필요한 사실을 검증할 수 있는 구조가 미래 신뢰 기술의 방향이다.
AI가 판단을 보조하는 경우에도 마찬가지다.
AI가 모든 원본을 항상 분석하는 것이 아니라, 필요한 순간에 필요한 신호만 검토하는 방향이 더 안전하다.
필요한 순간에만 검증 가능하게 하는 구조는 사생활을 보호하면서도 신뢰를

만든다.
이것이 기록 사회에서 가장 중요한 균형점 중 하나다.
6.7 원본 공개보다 판단값 제공을 우선한다
일곱 번째 원칙은 원본 공개보다 판단값 제공을 우선한다는 것이다.
원본 정보는 많은 내용을 담고 있지만, 항상 원본 전체가 필요한 것은 아니다.
오히려 원본 전체를 공개하면 불필요한 사생활 침해와 유출 위험이 생길 수 있다.
판단값은 원본에서 필요한 의미만 구조화한 결과다.
위험 점수, 신뢰 점수, 확인 필요, 추가 검토, 이상 신호, PASS/HOLD/STOP과 같은 상태값은 원본 전체를 공개하지 않고도 사용자가 판단할 수 있게 돕는다.
예를 들어 부동산 계약 전 위험 판단에서 사용자가 반드시 모든 법률 문서와 원본 기록을 직접 해석할 필요는 없다.
중요한 것은 다음 질문에 답하는 것이다.
어떤 항목이 위험 신호인가.
무엇을 추가 확인해야 하는가.
계약을 바로 진행해도 되는가.
전문가 상담이 필요한가.
계약을 보류해야 하는가.
판단값은 사용자의 의사결정을 돕는다.
다만 판단값은 법률 판단이나 절대적 확정을 의미하지 않는다.
판단값은 위험 신호를 이해 가능한 형태로 바꾸는 보조 신호다.
AI는 판단값 제공을 도울 수 있다.
그러나 AI가 생성한 판단값은 근거와 한계를 함께 제시해야 한다. 사용자는 AI 판단을 최종 결론이 아니라 판단 보조 신호로 이해해야 한다.
원본 공개보다 판단값 제공을 우선하면 두 가지 효과가 있다.
첫째, 민감한 정보 노출을 줄일 수 있다.
둘째, 사용자가 복잡한 정보를 쉽게 이해할 수 있다.
미래 신뢰 기술은 원본을 많이 보여주는 기술이 아니라, 필요한 판단을 안전하게 제공하는 기술이어야 한다.
6.8 사용자의 통제권을 보장한다
여덟 번째 원칙은 사용자의 통제권을 보장한다는 것이다.
기록은 사용자와 분리되어 존재해서는 안 된다.
사용자는 자신의 기록이 어떤 목적으로 수집되고, 어떻게 처리되며, 얼마나 보

관되고, 누구에게 제공되는지 알 수 있어야 한다.
사용자는 가능한 범위에서 자신의 기록에 대해 선택할 수 있어야 한다.
기록 제공 여부, 저장 여부, 삭제 여부, 리포트 생성 여부, 공유 여부를 통제할 수 있어야 한다.
사용자 통제권이 없는 기록 시스템은 신뢰를 만들기 어렵다.
사용자가 자신의 정보가 어떻게 쓰이는지 알 수 없다면, 그 시스템은 편리할 수는 있어도 신뢰받기 어렵다.
특히 민감한 기록일수록 사용자 통제권은 중요하다.
계약 정보, 신원 정보, 금융 정보, 의료 정보, 사적 대화, 위치 기록은 사용자의 삶과 직결된다.
AI 기반 시스템에서도 사용자 통제권은 반드시 필요하다.
사용자는 자신의 기록이 AI 분석에 사용되는지, 어떤 판단값이 생성되는지, 그 결과가 어디에 활용되는지 알 수 있어야 한다.
사용자 통제권은 단순한 설정 메뉴가 아니다.
그것은 기록 사회에서 인간의 자기결정권을 보호하는 장치다.
기록이 인간을 보호하기 위해 존재한다면, 인간은 자신의 기록에 대해 최소한의 통제권을 가져야 한다.
6.9 기록은 감시가 아니라 보호를 위해 존재해야 한다
아홉 번째 원칙은 기록은 감시가 아니라 보호를 위해 존재해야 한다는 것이다.
이 원칙은 신뢰 기록 최소화 원칙의 핵심이다.
기록은 사람을 통제하기 위해 존재해서는 안 된다.
기록은 사람을 위축시키고, 침묵하게 만들고, 항상 평가받는 대상으로 만들기 위해 존재해서는 안 된다.
기록은 사람이 위험을 피하도록 돕기 위해 존재해야 한다.
기록은 억울함을 줄이고, 사기와 조작을 막고, 계약과 거래의 책임을 분명히 하며, 사용자가 스스로를 보호할 수 있도록 존재해야 한다.
감시를 위한 기록과 보호를 위한 기록은 다르다.
감시를 위한 기록은 사람을 대상으로 본다.
보호를 위한 기록은 사람을 주체로 본다.
감시를 위한 기록은 권력이 기록을 소유한다.
보호를 위한 기록은 사용자가 기록의 의미와 범위를 이해하고 통제할 수 있게 한다.
감시를 위한 기록은 더 많이 보려고 한다.
보호를 위한 기록은 필요한 것만 보려고 한다.

AI 역시 감시가 아니라 보호를 위해 사용되어야 한다.
AI는 사람을 분류하고 통제하기 위한 최종 권한이 아니라, 위험 신호를 발견하고 사용자가 더 안전하게 판단하도록 돕는 보조 도구여야 한다.
미래 신뢰 기술은 감시 기술이 되어서는 안 된다.
미래 신뢰 기술은 보호 기술이어야 한다.
기록은 문명의 기억이다.
그러나 그 기억은 인간을 억압하기 위해서가 아니라, 인간이 더 안전하게 살아가기 위해 존재해야 한다.

7. 기록과 신뢰 판단 구조

기록은 단순히 과거를 보관하는 장치가 아니다.
기록은 현재의 판단을 가능하게 하는 근거가 된다.
그러나 기록이 많다고 해서 판단이 좋아지는 것은 아니다.
판단에는 정보의 양보다 정보의 구조가 중요하다.
기록은 흩어진 상태로 존재할 때 단순한 자료에 머문다. 하지만 기록이 목적에 맞게 분류되고, 위험 신호로 해석되고, 사용자가 이해 가능한 판단값으로 변환될 때 신뢰 판단의 근거가 된다.
본 장에서는 기록이 어떻게 신뢰 판단으로 연결되는지, 그리고 그 과정에서 원본 정보와 판단값을 어떻게 구분해야 하는지를 정의한다.
7.1 기록은 단순 저장이 아니라 판단의 근거가 된다
기록은 단순한 저장물이 아니다.
기록은 과거의 행위를 현재의 판단 근거로 바꾸는 장치다. 계약서가 남아 있으면 계약 내용을 판단할 수 있고, 거래 내역이 남아 있으면 돈의 흐름을 판단할 수 있으며, 인증 기록이 남아 있으면 행위의 권한을 판단할 수 있다.
기록은 판단을 가능하게 한다.
그러나 기록 자체가 곧 판단은 아니다.
기록은 자료다.
판단은 그 자료를 해석하는 과정이다.
예를 들어 부동산 계약에서 등기부등본, 보증금, 실거래가, 계약서, 중개 설명, 입금 요청, 계약 압박 신호는 각각 하나의 기록 또는 정보가 될 수 있다.
그러나 사용자는 이 기록들을 모두 보더라도 무엇이 위험한지 판단하기 어려

울 수 있다. 문제는 정보가 없는 것이 아니라, 정보가 판단으로 연결되지 않는 데 있다.
따라서 신뢰 기술은 기록을 단순히 저장하는 데 머물러서는 안 된다. 기록을 구조화하고, 위험 신호를 분류하고, 사용자가 이해할 수 있는 판단 근거로 바꾸어야 한다.
기록은 저장될 때 자료가 되고, 해석될 때 의미가 되며, 구조화될 때 판단의 근거가 된다.
7.2 신뢰 판단에는 원본 정보보다 구조화된 신호가 중요하다
신뢰 판단에는 원본 정보보다 구조화된 신호가 중요하다.
원본 정보는 많은 내용을 담고 있지만, 사용자가 그 내용을 모두 해석하기는 어렵다. 계약서 원본, 등기부등본, 실거래가 자료, 대화 내용, 인증 기록은 각각 의미가 있지만, 사용자가 그 의미를 종합해 판단하기는 쉽지 않다.
신뢰 판단에서 중요한 것은 원본 전체를 보여주는 것이 아니다.
중요한 것은 원본 안에서 판단에 필요한 신호를 찾아내는 것이다.
예를 들어 부동산 계약에서 중요한 신호는 다음과 같을 수 있다.
소유자와 계약 상대가 일치하는가.
근저당이나 압류 등 권리관계 위험이 있는가.
보증금이 시세 대비 과도한가.
보증보험 가입 가능성이 확인되었는가.
계약금 입금을 급하게 요구하는가.
설명이 계약서 내용과 일치하는가.
확인되지 않은 정보가 많은가.
이러한 신호는 원본 정보 전체보다 사용자의 의사결정에 직접적으로 도움이 된다.
구조화된 신호는 사용자가 놓치기 쉬운 위험을 보이게 만든다.
구조화된 신호는 복잡한 정보를 판단 가능한 형태로 바꾼다.
따라서 미래 신뢰 기술은 원본 정보를 많이 모으는 것에 머물러서는 안 된다. 원본에서 필요한 신호를 추출하고, 그 신호를 구조화해 판단값으로 연결해야 한다.
7.3 판단값과 원본 정보는 구분되어야 한다
판단값과 원본 정보는 구분되어야 한다.
원본 정보는 사건, 계약, 거래, 대화, 행위의 세부 내용을 담고 있다. 판단값은 그 원본 정보에서 특정 목적에 필요한 의미를 추출해 구조화한 결과다.
예를 들어 계약서 원본은 원본 정보다.

그 계약서에서 “특약 확인 필요”, “위험 조항 가능성”, “전문가 검토 권장”이라는 결과가 나왔다면 그것은 판단값이다.
등기부등본은 원본 정보다.
그 안에서 “근저당 확인 필요”, “소유자 일치 여부 확인 필요”라는 결과가 나왔다면 그것은 판단값이다.
사용자 입력값도 원본에 가까울 수 있다.
그 입력을 바탕으로 산출된 Trust Score, PASS/HOLD/STOP, 위험 신호 요약, 행동 가이드는 판단값이다.
판단값은 원본 전체를 대체하지 않는다.
판단값은 원본을 사용자가 이해 가능한 형태로 요약하고 해석한 보조 결과다.
이 구분은 중요하다.
판단값을 원본처럼 다루면 과도한 확정이 된다.
원본을 판단값처럼 다루면 민감한 정보가 과도하게 공개될 수 있다.
따라서 신뢰 기술은 원본 정보와 판단값을 명확히 분리해야 한다.
원본은 보호되어야 한다.
판단값은 설명 가능해야 한다.
사용자는 판단값의 의미와 한계를 이해할 수 있어야 한다.
7.4 신뢰 판단은 확정이 아니라 위험 신호의 구조화다
신뢰 판단은 확정이 아니다.
어떤 계약이 100% 안전하다고 단정할 수는 없다.
어떤 사람이 100% 신뢰할 수 있다고 확정할 수도 없다.
어떤 기록이 모든 진실을 완전히 설명한다고 말할 수도 없다.
현실의 판단은 언제나 불확실성을 가진다.
따라서 신뢰 판단의 역할은 절대적 확정이 아니라, 위험 신호를 구조화하는 것이다.
신뢰 판단은 다음과 같은 질문에 답해야 한다.
현재 어떤 위험 신호가 보이는가.
어떤 항목이 확인되지 않았는가.
어떤 정보가 추가로 필요한가.
어떤 경우에 계약을 보류해야 하는가.
어떤 경우에 전문가 상담이 필요한가.
어떤 경우에 사용자가 더 신중해야 하는가.
이러한 판단은 사용자의 의사결정을 돕는다.
그러나 사용자의 최종 결정을 대신하지 않는다.

Trust Score는 위험 신호의 구조화된 표현일 수 있다.
PASS/HOLD/STOP은 행동 방향을 정리한 보조 신호일 수 있다.
그러나 그것은 법률 판단이나 안전 보장을 의미하지 않는다.
신뢰 판단은 위험을 없애는 기술이 아니다.
신뢰 판단은 위험을 보이게 하는 기술이다.
위험을 보이게 만들면 사용자는 더 나은 선택을 할 수 있다.
이것이 신뢰 판단의 역할이다.
7.5 기록 기반 판단은 책임과 한계를 함께 가져야 한다
기록 기반 판단은 책임과 한계를 함께 가져야 한다.
기록을 바탕으로 판단값을 제공하는 시스템은 사용자에게 영향을 미친다. 그 판단값은 사용자의 행동, 선택, 계약, 거래, 상담 여부에 영향을 줄 수 있다.
따라서 판단 시스템은 자신이 무엇을 할 수 있고, 무엇을 할 수 없는지 명확히 해야 한다.
기록 기반 판단은 위험 신호를 구조화할 수 있다.
기록 기반 판단은 추가 확인이 필요한 항목을 보여줄 수 있다.
기록 기반 판단은 사용자가 놓치기 쉬운 요소를 알려줄 수 있다.
그러나 기록 기반 판단은 모든 위험을 제거할 수 없다.
기록 기반 판단은 법률 전문가의 판단을 대체할 수 없다.
기록 기반 판단은 실제 계약의 안전을 보장할 수 없다.
기록 기반 판단은 원본 정보의 오류나 누락까지 완전히 해결할 수 없다.
따라서 기록 기반 판단은 항상 설명과 한계를 함께 제공해야 한다.
판단값이 나온 이유를 설명해야 한다.
어떤 신호가 반영되었는지 알려야 한다.
어떤 정보가 부족한지 보여야 한다.
사용자가 다음에 무엇을 확인해야 하는지 안내해야 한다.
책임 있는 신뢰 기술은 확신을 과장하지 않는다.
책임 있는 신뢰 기술은 불확실성을 숨기지 않는다.
책임 있는 신뢰 기술은 사용자가 더 안전하게 판단하도록 돕는다.
7.6 Trust Score와 같은 판단값의 철학적 의미
Trust Score와 같은 판단값은 단순한 점수가 아니다.
Trust Score는 흩어진 위험 신호를 사용자가 이해할 수 있는 형태로 구조화한 결과다. 이는 기록과 정보의 양을 줄여 하나의 판단 가능한 상태값으로 바꾸는 방식이다.
Trust Score의 철학적 의미는 세 가지다.

첫째, 복잡한 정보를 이해 가능한 형태로 바꾼다.
사용자는 등기부, 보증금, 시세, 계약서, 설명 내용, 행동 신호를 모두 따로 이해하기 어려울 수 있다. Trust Score는 이러한 신호를 종합해 현재 상태를 직관적으로 보여준다.
둘째, 위험을 보이게 만든다.
위험은 항상 눈에 띄는 형태로 나타나지 않는다. 어떤 위험은 여러 작은 신호가 겹칠 때 나타난다. Trust Score는 흩어진 신호를 모아 사용자가 위험을 인식하게 돕는다.
셋째, 판단을 보조하되 확정하지 않는다.
Trust Score는 “안전 보장”이 아니다. Trust Score는 “현재 입력된 정보와 확인된 신호를 기준으로 볼 때 어느 정도의 주의가 필요한가”를 보여주는 판단 보조값이다.
따라서 Trust Score는 단순한 기술적 출력값이 아니라, 기록 사회에서 복잡한 정보를 인간이 이해 가능한 판단값으로 바꾸는 철학적 장치다.
Trust Score는 원본을 많이 드러내기보다, 필요한 위험 신호를 구조화해 사용자에게 돌려주는 방식이어야 한다.
이 점에서 Trust Score는 신뢰 기록 최소화 원칙과 연결된다.
7.7 PASS/HOLD/STOP과 같은 행동 판단의 의미
PASS/HOLD/STOP과 같은 행동 판단은 사용자의 다음 행동을 돕기 위한 상태 분류다.
PASS는 현재 입력된 정보와 확인된 신호를 기준으로 상대적으로 큰 위험 신호가 낮은 상태를 의미한다. 그러나 PASS는 안전 보장을 의미하지 않는다. PASS는 “현재 기준으로 큰 경고 신호는 낮지만, 기본 확인은 계속 필요하다”는 보조 판단이다.
HOLD는 추가 확인이 필요한 상태를 의미한다. HOLD는 불확실성이 있거나, 일부 위험 신호가 확인되었거나, 사용자가 놓친 항목이 있을 수 있음을 뜻한다. 이 상태에서는 계약을 바로 진행하기보다 추가 서류 확인, 설명 요청, 보증 가능 여부 확인, 전문가 상담을 검토해야 한다.
STOP은 강한 위험 신호가 감지되었거나, 계약 진행을 보류해야 할 가능성이 큰 상태를 의미한다. STOP은 사용자가 즉시 계약을 중단하라는 법률 명령이 아니라, 매우 신중한 검토와 전문가 상담이 필요한 경고 신호다.
PASS/HOLD/STOP의 의미는 단순한 등급 분류가 아니다.
그것은 사용자의 행동을 정리해주는 판단 언어다.
복잡한 위험 정보를 사용자가 바로 이해하기는 어렵다.

그러나 PASS/HOLD/STOP은 사용자가 다음 질문을 하도록 만든다.
지금 진행해도 되는가.
무엇을 더 확인해야 하는가.
잠시 멈춰야 하는가.
전문가에게 물어봐야 하는가.
이러한 행동 판단은 기록을 사용자 보호로 연결하는 장치다.
기록은 자료에 머물러서는 안 된다.
기록은 신호가 되어야 하고, 신호는 판단값이 되어야 하며, 판단값은 사용자가 더 안전한 행동을 선택하도록 도와야 한다.
PASS/HOLD/STOP은 바로 그 연결 구조의 언어다.
7.8 AI는 기록을 판단 신호로 변환할 수 있지만, 판단의 최종 책임이 되어서는 안 된다
AI는 기록을 판단 가능한 신호로 변환하는 데 도움을 줄 수 있다.
사람은 많은 기록을 한 번에 해석하기 어렵다. 계약서, 등기부등본, 실거래가, 대화 내용, 인증 기록, 거래 내역, 설명 자료가 동시에 존재할 때 일반 사용자는 무엇이 중요한 위험 신호인지 놓치기 쉽다.
AI는 이러한 흩어진 기록을 분석하고, 핵심 문장을 요약하고, 이상 패턴을 발견하고, 위험 가능성이 있는 항목을 분류할 수 있다.
이 점에서 AI는 기록 기반 신뢰 판단의 보조 도구가 될 수 있다.
그러나 AI가 판단의 최종 책임이 되어서는 안 된다.
AI는 기록의 맥락을 완전히 이해하지 못할 수 있다.
AI는 잘못된 입력값을 바탕으로 잘못된 결론을 낼 수 있다.
AI는 편향된 데이터에 영향을 받을 수 있다.
AI는 그럴듯하지만 부정확한 설명을 생성할 수 있다.
AI는 불확실성을 확정처럼 표현할 수 있다.
따라서 AI 기반 판단은 반드시 한계를 가져야 한다.
AI는 위험 신호를 발견하고 정리할 수 있다.
그러나 AI는 사용자의 계약 안전을 보장할 수 없다.
AI는 법률 전문가의 판단을 대체할 수 없다.
AI는 인간의 최종 의사결정을 대신할 수 없다.
AI의 역할은 판단의 주체가 아니라 판단의 보조자여야 한다.
AI가 제공해야 하는 것은 단정이 아니라 근거다.
AI가 제공해야 하는 것은 확정이 아니라 위험 신호의 구조화다.
AI가 제공해야 하는 것은 명령이 아니라 사용자가 다음 행동을 선택할 수 있

는 판단 보조값이다.
따라서 AI 기반 신뢰 판단은 다음 원칙을 따라야 한다.
원본 정보는 보호한다.
필요한 신호만 추출한다.
판단 근거를 설명한다.
불확실성을 숨기지 않는다.
사용자에게 최종 판단 권한을 남긴다.
전문가 상담이 필요한 경우 이를 명확히 안내한다.
AI는 기록을 해석할 수 있다.
그러나 기록을 해석하는 권한은 인간 보호의 원칙 안에 있어야 한다.
AI는 신뢰 판단의 보조자가 될 수 있다.
그러나 신뢰의 최종 책임은 인간과 사회적 검증 구조 안에 남아 있어야 한다.

8. 믿집과의 연결

기록의 양면성 원리와 신뢰 기록 최소화 원칙은 믿집의 서비스 철학과 직접적으로 연결된다.
믿집은 단순히 부동산 계약 정보를 저장하는 서비스가 아니다.
믿집은 계약 전 사용자가 놓치기 쉬운 위험 신호를 구조화하고, 그 신호를 사용자가 이해 가능한 판단값으로 변환하는 서비스다.
부동산 계약에서 문제는 정보가 전혀 없다는 데만 있지 않다. 등기부등본, 보증금, 시세, 소유자 정보, 계약서, 특약, 중개 설명, 입금 요청, 보증보험 가능 여부 등 확인해야 할 정보는 이미 여러 곳에 존재한다.
문제는 이 정보들이 흩어져 있고, 사용자가 이를 종합해 계약 진행 여부로 연결하기 어렵다는 점이다.
믿집은 이 지점에서 작동한다.
믿집은 모든 정보를 저장하려는 서비스가 아니라, 계약 전 위험 판단에 필요한 최소 신호를 구조화하고, Trust Score와 PASS/HOLD/STOP 판단값을 통해 사용자가 더 안전하게 의사결정하도록 돕는 신뢰 점수 엔진이어야 한다.

8.1 믿집은 모든 계약 정보를 저장하는 서비스가 아니다

믿집은 사용자의 모든 계약 정보를 저장하는 서비스가 아니다.
부동산 계약 정보는 매우 민감하다. 계약서에는 이름, 주소, 보증금, 월세, 계좌, 서명, 계약 조건, 특약, 임대인과 임차인의 관계 정보가 포함될 수 있다.
이러한 정보를 무분별하게 저장하는 것은 사용자 보호가 아니라 새로운 위험을 만드는 일이 될 수 있다.
믿집의 방향은 사용자의 계약 원본을 많이 보유하는 데 있지 않다.

믿집의 방향은 계약 전 사용자가 직접 확인해야 할 위험 신호를 쉽게 이해하도록 돕는 데 있다.
따라서 믿집은 초기 단계에서 개인정보나 계약서 원본을 저장하지 않는 방향으로 설계되어야 한다. 사용자가 입력한 조건과 위험 신호가 브라우저 안에서 분석되어 Trust Score와 PASS/HOLD/STOP 결과로 변환되는 방식은 이러한 철학과 연결된다.
믿집은 “많이 저장하는 서비스”가 아니라 “필요한 위험 신호만 판단하는 서비스”여야 한다.
이것이 기록의 양면성 원리에서 믿집이 가져야 할 첫 번째 원칙이다.
8.2 믿집은 계약 전 위험 신호를 구조화하는 서비스다
믿집은 계약 전 위험 신호를 구조화하는 서비스다.
부동산 계약에서 위험은 하나의 정보로만 드러나지 않는다.
여러 작은 신호가 함께 나타날 때 위험이 커질 수 있다.
예를 들어 등기부등본을 확인하지 않았다는 사실 하나만으로 모든 계약이 위험하다고 단정할 수는 없다. 그러나 소유자 일치 여부가 불분명하고, 근저당 확인이 되지 않았으며, 계약금 입금을 급하게 요구하고, 설명과 서류 제공이 지연된다면 위험 신호는 훨씬 커진다.
믿집은 이러한 흩어진 신호를 하나의 판단 구조로 묶어야 한다.
계약 전 위험 신호에는 다음과 같은 요소가 포함될 수 있다.
소유자 일치 여부.
권리관계 확인 여부.
근저당·압류·가압류 등 권리 제한 가능성.
보증금 구조와 시세 대비 위험성.
선순위 보증금 여부.
전세보증금 반환보증 가능성.
계약서와 설명 내용의 불일치.
대리인 계약 여부.
계약금 입금 재촉.
서류 제공 회피.
설명 회피.
확인되지 않은 정보의 누적.
믿집의 역할은 이 신호들을 사용자가 이해 가능한 형태로 정리하는 것이다.
따라서 믿집은 단순 체크리스트가 아니다.
믿집은 계약 전 위험 신호를 구조화해 사용자의 판단을 돕는 신뢰 판단 보조

시스템이다.

8.3 믿집에서 기록되어야 할 것과 기록되지 말아야 할 것

믿집은 기록되어야 할 것과 기록되지 말아야 할 것을 구분해야 한다.

기록되어야 할 것은 사용자의 보호와 서비스 개선에 필요한 최소 정보다. 예를 들어 사용자가 어떤 유형의 위험 신호에서 어려움을 겪는지, 어떤 결과 화면을 이해하기 쉬워하는지, PASS/HOLD/STOP 판단이 도움이 되었는지, 어떤 개선 의견이 있었는지는 비식별 형태로 수집될 수 있다.

또한 사용자가 원할 경우, 사용자가 직접 내려받는 형태의 리포트나 체크리스트는 생성될 수 있다. 이때도 사용자의 동의와 통제권이 전제되어야 한다.

반대로 기록되지 말아야 할 것은 불필요한 민감 원본 정보다.

정확한 주소, 계약서 원본, 임대인 이름, 임차인 실명, 계좌번호, 주민등록번호, 신분증, 서명 원본, 사적인 대화 전체 등은 초기 MVP 단계에서 저장 대상이 되어서는 안 된다.

믿집이 다루어야 할 핵심은 원본의 축적이 아니라 위험 신호의 구조화다.

따라서 믿집은 다음 원칙을 가져야 한다.

위험 판단에 필요한 최소 신호만 입력받는다.

민감한 원본 정보는 저장하지 않는다.

사용자 테스트 데이터는 익명·비식별 형태로 다룬다.

서비스 개선 목적이 끝난 정보는 최소화한다.

사용자가 원하지 않는 기록은 남기지 않는다.

사용자가 결과를 복사하거나 저장할지 선택할 수 있게 한다.

기록의 목적은 서비스가 사용자를 더 많이 아는 것이 아니라, 사용자가 자신의 위험을 더 잘 이해하도록 돕는 것이다.

8.4 개인정보·계약서 원본·정확한 주소 저장 최소화 원칙

믿집은 개인정보, 계약서 원본, 정확한 주소 저장을 최소화해야 한다.

부동산 계약 위험 판단에서 정확한 주소와 계약서 원본은 매우 강한 정보다. 그만큼 유출될 경우 피해도 크다.

정확한 주소는 사용자의 거주지와 생활권을 드러낼 수 있다.

계약서 원본은 보증금, 월세, 특약, 임대인과 임차인의 이름, 서명, 계약 관계를 드러낼 수 있다.

개인정보는 금융 사기, 신분 도용, 협박, 스토킹 등 다양한 위험으로 이어질 수 있다.

따라서 믿집은 초기 단계에서 이러한 원본 정보를 서버에 저장하지 않는 방향으로 설계되어야 한다.

위험 판단은 반드시 모든 원본을 저장해야만 가능한 것이 아니다. 사용자가 직접 선택한 위험 신호, 확인 여부, 모르겠음 응답, 계약 유형, 보증금 범위, 계약 압박 여부만으로도 1차적 판단 보조는 가능하다.
향후 공공데이터와 연동하더라도, 우선적으로는 도로명주소, 건축물대장, 실거래가 등 공개·공공데이터의 연동 가능성을 검토하는 방향이 안전하다. 민감한 계약서 원본 분석은 사용자의 명시적 동의, 저장 최소화, 처리 후 삭제, 권한 통제, 보안 정책이 갖추어진 이후에 제한적으로 검토되어야 한다.
믿집의 신뢰는 많은 개인정보를 보유하는 데서 나오지 않는다.
믿집의 신뢰는 필요한 신호만 안전하게 판단하는 구조에서 나온다.
8.5 Trust Score는 위험 신호를 사용자가 이해하도록 돕는 판단값이다
Trust Score는 위험 신호를 사용자가 이해하도록 돕는 판단값이다.
Trust Score는 안전을 보장하는 숫자가 아니다.
Trust Score는 현재 입력된 조건과 확인된 위험 신호를 바탕으로, 사용자가 계약 전 상태를 더 쉽게 이해하도록 돕는 구조화된 결과값이다.
부동산 계약에서 사용자는 여러 정보를 접한다. 그러나 그 정보가 많다고 해서 사용자가 더 좋은 판단을 하는 것은 아니다.
등기부등본을 봐도 무엇을 확인해야 하는지 모를 수 있다.
보증금이 적정한지 판단하기 어려울 수 있다.
상대방의 설명이 서류와 일치하는지 놓칠 수 있다.
계약을 서두르는 상황이 위험 신호인지 판단하지 못할 수 있다.
Trust Score는 이런 흩어진 위험 신호를 사용자가 이해 가능한 형태로 바꾼다.
Trust Score의 목적은 사용자를 대신해 결론을 내려주는 것이 아니다.
Trust Score의 목적은 사용자가 현재 상황을 더 잘 보게 하는 것이다.
따라서 Trust Score는 항상 설명 가능한 방식으로 제공되어야 한다.
점수만 제공해서는 안 된다.
왜 점수가 낮아졌는지, 어떤 항목이 위험 신호로 반영되었는지, 무엇을 추가 확인해야 하는지가 함께 제공되어야 한다.
Trust Score는 기록을 판단값으로 바꾸는 장치다.
그리고 그 판단값은 사용자의 보호를 위해 존재해야 한다.
8.6 PASS/HOLD/STOP은 법률 판단이 아니라 행동 보조 신호다
PASS/HOLD/STOP은 법률 판단이 아니라 행동 보조 신호다.
PASS는 현재 입력된 정보와 확인된 위험 신호 기준으로 상대적으로 큰 경고 신호가 낮은 상태를 의미한다. 그러나 PASS는 계약의 안전을 보장하지 않는

다. 기본적인 서류 확인과 최종 검토는 여전히 필요하다.
HOLD는 추가 확인이 필요한 상태를 의미한다. 확인되지 않은 정보가 있거나, 일부 위험 신호가 존재하거나, 사용자가 더 신중하게 살펴봐야 할 항목이 있다는 뜻이다. HOLD 상태에서는 계약을 바로 진행하기보다 추가 서류 확인, 보증 가능 여부 확인, 설명 요청, 전문가 상담을 검토해야 한다.
STOP은 강한 위험 신호가 감지되었거나, 계약 진행을 보류해야 할 가능성이 높은 상태를 의미한다. STOP은 법적 명령이 아니라 경고 신호다. 이 상태에서는 계약금 입금이나 서명 전에 전문가 상담과 추가 검토가 필요하다.
PASS/HOLD/STOP은 사용자의 행동을 정리해주는 언어다.
복잡한 위험 정보를 사용자가 한 번에 이해하기는 어렵다.
그러나 PASS/HOLD/STOP은 사용자가 다음 질문을 할 수 있게 만든다.
지금 진행해도 되는가.
무엇을 더 확인해야 하는가.
잠시 멈춰야 하는가.
전문가에게 물어봐야 하는가.
따라서 PASS/HOLD/STOP은 법률 판단을 대체하지 않는다.
그것은 사용자가 계약 전 단계에서 더 안전한 행동을 선택하도록 돕는 판단 보조 신호다.
8.7 믿집은 감시 시스템이 아니라 보호 시스템이어야 한다
믿집은 감시 시스템이 아니라 보호 시스템이어야 한다.
믿집의 목적은 사용자의 정보를 많이 모으는 것이 아니다.
믿집의 목적은 사용자가 계약 전 위험을 놓치지 않도록 돕는 것이다.
감시 시스템은 사람을 대상으로 본다.
보호 시스템은 사람을 주체로 본다.
감시 시스템은 더 많은 정보를 보려고 한다.
보호 시스템은 필요한 정보만 보려고 한다.
감시 시스템은 기록을 소유하려 한다.
보호 시스템은 사용자가 기록의 의미와 범위를 이해하고 통제하도록 돕는다.
믿집은 보호 시스템이어야 한다.
믿집은 사용자가 놓치기 쉬운 위험 신호를 보여주고, 추가 확인이 필요한 항목을 안내하며, 계약을 서두르지 않도록 돕고, 필요한 경우 전문가 상담을 유도해야 한다.
믿집은 사용자를 감시하는 서비스가 아니라, 사용자가 스스로를 보호할 수 있도록 돕는 서비스여야 한다.

기록은 믿집에서 통제의 도구가 아니라 보호의 도구가 되어야 한다.
이것이 기록의 양면성 원리와 신뢰 기록 최소화 원칙이 믿집에 주는 가장 중요한 방향이다.

9. DET와의 연결

DET, 즉 디지털 실존 증명은 기록의 양면성 원리와 깊게 연결된다.
디지털 사회에서는 사람이 실제로 존재했는지, 어떤 행위를 했는지, 어떤 권한으로 승인했는지, 어떤 시점에 어떤 선택을 했는지를 증명해야 하는 상황이 많아진다.
그러나 디지털 실존을 증명한다는 이유로 개인의 모든 행위를 노출해서는 안 된다. 실존 증명은 감시로 변질될 위험을 항상 갖고 있다.
따라서 DET는 무차별적인 기록 공개가 아니라, 필요한 순간에 필요한 사실만 검증하는 구조 위에서 설계되어야 한다.
DET의 핵심은 인간을 더 많이 노출시키는 것이 아니라, 인간이 필요한 사실만 안전하게 증명할 수 있도록 돕는 데 있다.
9.1 디지털 실존 증명이 필요한 이유
디지털 실존 증명이 필요한 이유는 디지털 사회에서 진짜와 가짜를 구분하기 점점 어려워지고 있기 때문이다.
AI 생성물, 딥페이크, 합성 음성, 자동화 계정, 허위 신원, 위조 문서, 조작된 기록은 디지털 환경에서 신뢰를 흔든다.
누가 실제로 말했는가.
누가 실제로 승인했는가.
그 사람이 실제로 존재하는가.
그 행위가 실제 당사자의 의사였는가.
그 기록은 언제 생성되었는가.
그 기록은 조작되지 않았는가.
이 질문은 앞으로 더 중요해질 것이다.
디지털 사회에서 실존은 단순히 살아 있는 사람이라는 의미를 넘는다. 디지털 실존은 특정 시점에 특정 주체가 실제로 존재했고, 특정 행위를 했으며, 그 행위가 조작되거나 위조되지 않았다는 신뢰의 문제와 연결된다.
계약, 금융, 인증, 창작, 투표, 행정, 의료, 법률, 플랫폼 활동에서 디지털 실존 증명은 점점 더 중요해질 수 있다.
따라서 DET는 디지털 사회에서 사람과 행위의 진위를 확인하기 위한 신뢰 기

반으로 제안될 수 있다.
그러나 그 증명은 반드시 사생활 보호와 함께 설계되어야 한다.
9.2 디지털 실존 증명과 사생활 보호의 충돌
디지털 실존 증명은 사생활 보호와 충돌할 수 있다.
어떤 사람이 실제로 존재했는지, 어떤 행위를 했는지 증명하려면 기록이 필요하다. 그러나 그 기록이 지나치게 많이 공개되면 개인의 사생활이 침해될 수 있다.
예를 들어 어떤 사용자가 특정 계약에 동의했는지를 증명해야 할 수 있다. 그러나 이를 위해 사용자의 모든 위치 기록, 전체 대화 기록, 모든 접속 이력, 전체 신분 정보를 공개할 필요는 없다.
디지털 실존 증명이 과도하게 설계되면 감시 체계가 될 수 있다. 사람의 모든 행동을 기록하고, 모든 행동을 검증 가능하게 만들고, 모든 활동을 추적한다면 그것은 신뢰 기술이 아니라 통제 기술이 될 위험이 있다.
따라서 DET는 두 가지 요구 사이의 균형을 찾아야 한다.
첫째, 진짜를 증명해야 한다.
둘째, 인간을 과도하게 노출해서는 안 된다.
이 균형이 없다면 디지털 실존 증명은 신뢰의 기술이 아니라 감시의 기술로 오해받거나 변질될 수 있다.
DET는 실존을 증명하되, 인간의 전체 삶을 공개하지 않는 방향이어야 한다.
9.3 DET는 무차별 공개가 아니라 필요한 사실의 검증이어야 한다
DET는 무차별 공개가 아니라 필요한 사실의 검증이어야 한다.
디지털 실존을 증명한다고 해서 모든 기록을 보여줄 필요는 없다. 실존 증명의 목적은 사람의 전체 삶을 공개하는 것이 아니다. 목적은 특정 상황에서 필요한 사실을 확인하는 것이다.
예를 들어 다음과 같은 사실만 검증하면 충분할 수 있다.
해당 행위가 실제 사용자에 의해 승인되었는가.
해당 계정이 실제 사람과 연결되어 있는가.
해당 기록이 특정 시점 이후 조작되지 않았는가.
해당 창작물이 특정 주체로부터 생성되었는가.
해당 계약 행위가 권한 있는 주체에 의해 이루어졌는가.
이때 필요한 것은 전체 원본의 공개가 아니다.
필요한 것은 특정 사실의 검증이다.
DET는 이러한 방향으로 설계되어야 한다.
즉, DET는 “모든 것을 보여주는 증명”이 아니라 “필요한 것만 증명하는 구

조”여야 한다.
이 원칙은 신뢰 기록 최소화 원칙과 연결된다. DET는 기록을 통해 신뢰를 만들되, 기록이 인간을 해치지 않도록 필요한 범위 안에서만 검증되어야 한다.
디지털 실존 증명의 미래는 무차별 공개가 아니라 선택적 검증에 있다.
9.4 행위의 진위와 원본 사생활은 분리되어야 한다
DET에서 가장 중요한 원칙 중 하나는 행위의 진위와 원본 사생활을 분리하는 것이다.
어떤 행위가 진짜인지 확인해야 한다고 해서, 그 행위와 연결된 모든 사생활을 공개할 필요는 없다.
예를 들어 어떤 사용자가 계약서에 동의했는지 확인할 수 있어야 한다. 그러나 그 사용자의 모든 계약 이력, 전체 금융 상태, 전체 대화 기록, 전체 위치 기록을 공개할 필요는 없다.
어떤 창작물이 특정 시점에 특정 주체에 의해 생성되었는지 확인할 수 있어야 한다. 그러나 창작자의 모든 작업 과정과 사적 기록을 공개할 필요는 없다.
어떤 인증 행위가 실제 사용자에 의해 이루어졌는지 확인할 수 있어야 한다. 그러나 사용자의 모든 접속 이력과 생활 패턴을 공개할 필요는 없다.
행위의 진위는 검증되어야 한다.
그러나 원본 사생활은 보호되어야 한다.
이 분리는 디지털 사회에서 매우 중요하다.
분리가 없다면 실존 증명은 곧 사생활 공개가 된다.
분리가 있다면 실존 증명은 보호형 신뢰 기술이 될 수 있다.
DET는 바로 이 분리 원칙 위에서 설계되어야 한다.
9.5 선택적 검증 구조의 필요성
DET에는 선택적 검증 구조가 필요하다.
선택적 검증이란 전체 정보를 공개하지 않고도, 필요한 사실만 확인할 수 있는 구조를 의미한다.
디지털 사회에서 신뢰를 만들기 위해 모든 정보를 공개하는 방식은 위험하다. 그 방식은 신뢰를 만들 수는 있지만, 동시에 감시와 유출, 협박과 악용의 위험도 만든다.
선택적 검증 구조는 이 위험을 줄인다.
사용자는 필요한 사실만 증명할 수 있어야 한다.
시스템은 필요한 판단만 확인할 수 있어야 한다.
제3자는 필요 이상의 정보를 볼 수 없어야 한다.
예를 들어 “이 사용자가 실제 사람인가”를 확인할 때, 사용자의 전체 신분 정

보를 공개하지 않아도 된다.
“이 행위가 본인 승인인가”를 확인할 때, 사용자의 모든 활동 기록을 공개하지 않아도 된다.
“이 기록이 조작되지 않았는가”를 확인할 때, 원본 전체를 공개하지 않고도 무결성 여부를 검증할 수 있어야 한다.
선택적 검증 구조는 디지털 실존 증명을 인간 보호의 방향으로 이끈다.
DET가 신뢰 기술로 작동하려면 선택적 검증은 선택 사항이 아니라 핵심 조건이어야 한다.
9.6 DET와 신뢰 기록 최소화 원칙의 관계
DET는 신뢰 기록 최소화 원칙과 연결되어야 한다.
디지털 실존을 증명하기 위해 기록은 필요하다.
그러나 그 기록은 최소화되어야 한다.
DET는 모든 행위를 저장하는 구조가 되어서는 안 된다.
DET는 필요한 행위, 필요한 시점, 필요한 권한, 필요한 증명만 다루는 구조여야 한다.
신뢰 기록 최소화 원칙은 DET에 다음 방향을 제시한다.
모든 것을 기록하지 않는다.
필요한 사실만 검증한다.
민감한 원본 정보는 보호한다.
목적이 끝난 기록은 최소화한다.
권한 있는 주체만 접근하게 한다.
필요한 순간에만 검증 가능하게 한다.
원본 공개보다 증명값과 판단값 제공을 우선한다.
사용자의 통제권을 보장한다.
기록은 감시가 아니라 보호를 위해 존재해야 한다.
이 원칙은 DET가 감시 시스템으로 변질되지 않기 위한 안전장치다.
DET는 인간의 디지털 실존을 증명하는 기술일 수 있다. 그러나 그 증명은 인간을 더 많이 노출시키는 방향이 아니라, 인간을 더 안전하게 보호하는 방향이어야 한다.
DET의 신뢰는 얼마나 많은 기록을 보유하느냐에서 나오지 않는다.
DET의 신뢰는 필요한 사실만 안전하게 증명할 수 있는 구조에서 나온다.
9.7 디지털 실존은 감시가 아니라 신뢰의 기반이어야 한다
디지털 실존은 감시가 아니라 신뢰의 기반이어야 한다.
디지털 사회에서 사람과 행위의 진위를 확인하는 일은 점점 더 중요해질 것이

다. 그러나 진위를 확인한다는 명분으로 모든 사람의 모든 행위를 추적하는 사회가 되어서는 안 된다.
디지털 실존 증명은 인간을 통제하기 위한 기술이 아니다.
그것은 인간이 디지털 환경에서 위조, 조작, 사칭, 허위 기록으로부터 보호받기 위한 기술이어야 한다.
감시를 위한 디지털 실존은 위험하다.
그것은 인간을 끊임없이 관찰되는 대상으로 만든다.
신뢰를 위한 디지털 실존은 다르다.
그것은 인간이 필요한 순간에 자신과 자신의 행위를 안전하게 증명할 수 있도록 돕는다.
DET는 이 방향으로 설계되어야 한다.
DET는 사람의 모든 삶을 공개하는 기술이 아니라, 필요한 순간에 필요한 사실만 증명하는 기술이어야 한다.
DET는 감시의 기반이 아니라 신뢰의 기반이어야 한다.
DET는 통제의 도구가 아니라 보호의 도구여야 한다.
기록의 시대에 디지털 실존 증명은 피할 수 없는 흐름일 수 있다.
그러나 그 흐름은 인간을 더 많이 노출시키는 방향이 아니라, 인간을 더 안전하게 보호하는 방향으로 가야 한다.
이것이 기록의 양면성 원리와 신뢰 기록 최소화 원칙이 DET에 부여하는 철학적 기준이다.

10. 기존 개념과의 관계

본 문서에서 제안하는 기록의 양면성 원리와 신뢰 기록 최소화 원칙은 완전히 고립된 개념이 아니다.
이 문서는 기존에 존재해온 프라이버시 보호, 데이터 최소화, Privacy by Design, 선택적 공개, 영지식 증명, DID, 블록체인, 감사 로그, AI 신뢰·AI 거버넌스와 같은 개념들과 연결된다.
그러나 본 문서는 이러한 개념을 단순히 반복하거나 나열하는 데 목적이 있지 않다.
본 문서의 목적은 디지털 사회에서 기록이 신뢰를 만드는 동시에 위험을 만드는 구조를 상위 철학으로 정의하고, 기존 개념들을 신뢰 판단과 인간 보호의 관점에서 다시 연결하는 데 있다.
기존 개념들은 각각의 영역에서 중요한 역할을 해왔다.

프라이버시 보호는 개인의 권리와 사생활 보호를 강조했고, 데이터 최소화는 수집 범위를 줄이는 원칙을 제시했으며, Privacy by Design은 설계 단계에서 보호 원칙을 반영해야 한다고 보았다. 선택적 공개와 영지식 증명은 필요한 사실만 증명하는 기술적 방향을 제시했고, DID는 디지털 신원에 대한 사용자 주권을 강조했으며, 블록체인과 감사 로그는 기록의 위변조 방지와 추적 가능성을 강조했다. AI 신뢰와 AI 거버넌스는 인공지능이 어떤 기준으로 판단하고, 그 판단에 어떤 책임과 설명 구조가 필요한지를 다룬다.
본 문서는 이 모든 흐름을 하나의 질문 아래에서 다시 본다.
기록은 어떻게 신뢰가 되고, 어떻게 위험이 되는가.
기록은 무엇을 보호해야 하며, 무엇을 증명해야 하는가.
미래 신뢰 기술은 인간을 더 많이 노출시켜야 하는가, 아니면 필요한 사실만 안전하게 검증해야 하는가.
이 질문에 대한 본 문서의 답은 명확하다.
미래의 신뢰 기술은 더 많이 저장하는 기술이 아니라, 필요한 기록만 안전하게 구조화하고, 필요한 순간에만 검증 가능한 판단값을 제공하는 기술이어야 한다.
10.1 프라이버시 보호와의 관계
프라이버시 보호는 개인의 사생활과 자기결정권을 지키기 위한 핵심 개념이다.
프라이버시는 단순히 “숨길 권리”가 아니다.
프라이버시는 인간이 자신의 삶을 스스로 통제할 수 있는 권리와 연결된다.
개인의 대화, 위치, 건강, 금융, 관계, 감정, 소비, 행동 기록은 모두 그 사람의 삶을 설명할 수 있는 단서가 된다. 이러한 기록이 권한 없이 수집되거나 공개될 경우, 개인은 자신의 삶에 대한 통제권을 잃게 된다.
따라서 프라이버시 보호는 디지털 사회에서 인간 존엄의 기초다.
본 문서의 기록의 양면성 원리는 프라이버시 보호와 깊게 연결된다.
기록은 신뢰를 위해 필요할 수 있지만, 그 기록이 개인의 사생활을 침해하면 신뢰가 아니라 폭력이 된다.
프라이버시 보호의 핵심은 다음과 같다.
개인의 민감한 정보가 권한 없이 수집되지 않아야 한다.
수집된 정보는 목적에 맞게 제한적으로 사용되어야 한다.
개인은 자신의 정보가 어떻게 쓰이는지 알 수 있어야 한다.
불필요하거나 목적이 끝난 정보는 삭제되거나 최소화되어야 한다.
정보는 개인을 통제하기 위해 사용되어서는 안 된다.
본 문서는 여기에 한 가지 관점을 더한다.

프라이버시는 단순히 “보호해야 할 영역”이 아니라, 신뢰 기술이 반드시 지켜야 할 경계선이다.
즉, 신뢰를 만든다는 명분으로 프라이버시를 무너뜨려서는 안 된다.
사기를 막고, 계약을 검증하고, 행위의 진위를 확인하려는 목적이 있더라도, 인간의 전체 삶을 무차별적으로 노출하는 방식은 정당화될 수 없다.
따라서 본 문서는 프라이버시 보호를 신뢰 기술의 부가 기능이 아니라, 신뢰 기술의 기본 조건으로 본다.
기록이 인간을 보호하려면, 먼저 인간의 사생활을 침해하지 않아야 한다.
10.2 데이터 최소화와의 관계
데이터 최소화는 필요한 정보만 수집하고, 불필요한 정보는 수집하지 않는 원칙이다.
디지털 사회에서 많은 서비스와 시스템은 가능한 한 많은 데이터를 모으려는 방향으로 발전해왔다. 더 많은 데이터는 더 정교한 분석과 예측을 가능하게 한다. 그러나 동시에 더 많은 유출 위험, 더 많은 감시 가능성, 더 많은 악용 가능성을 만든다.
데이터 최소화는 이 위험을 줄이기 위한 핵심 원칙이다.
본 문서의 신뢰 기록 최소화 원칙은 데이터 최소화와 연결된다.
그러나 단순히 “덜 수집하자”는 주장에 머물지 않는다.
본 문서는 데이터 최소화를 신뢰 판단 구조의 핵심 원칙으로 확장한다.
즉, 데이터 최소화는 단순한 개인정보 보호 조치가 아니다.
데이터 최소화는 기록이 신뢰가 되기 위해 반드시 필요한 구조적 조건이다.
왜냐하면 신뢰는 데이터의 양에서 나오지 않기 때문이다.
신뢰는 필요한 데이터를 올바르게 수집하고, 안전하게 처리하며, 필요한 판단값으로 변환하는 구조에서 나온다.
예를 들어 부동산 계약 전 위험 판단에서 모든 계약 정보를 수집할 필요는 없다. 계약서 원본 전체, 신분증, 정확한 주소, 임대인 개인정보, 계좌정보를 모두 수집하지 않아도 1차적인 위험 신호 판단은 가능할 수 있다.
필요한 것은 목적에 맞는 최소 신호다.
소유자 일치 여부.
권리관계 확인 여부.
근저당 확인 여부.
보증금과 시세의 관계.
계약금 입금 압박.
설명 불일치.

확인되지 않은 정보의 누적.
이러한 신호는 원본 전체보다 더 안전하고, 사용자에게는 더 직접적인 판단 근거가 될 수 있다.
AI 기반 판단에서도 데이터 최소화는 더욱 중요하다.
AI는 많은 데이터를 처리할 수 있지만, 많은 데이터를 처리할 수 있다는 이유만으로 모든 데이터를 제공받아서는 안 된다. AI는 기록을 결합해 개인이 직접 공개하지 않은 사실까지 추론할 수 있기 때문이다.
따라서 본 문서는 데이터 최소화를 다음과 같이 재정의한다.
데이터 최소화는 단순히 데이터를 적게 받는 것이 아니라, 신뢰 판단에 필요한 신호만 남기고 인간을 해칠 수 있는 원본 노출을 줄이는 설계 원칙이다.
10.3 Privacy by Design과의 관계
Privacy by Design은 개인정보 보호를 서비스나 시스템의 사후 보완 기능으로 보는 것이 아니라, 설계 단계부터 포함해야 한다는 접근이다.
이는 매우 중요한 개념이다.
많은 시스템은 먼저 기능을 만들고, 나중에 개인정보 보호나 보안을 덧붙인다.
그러나 민감한 기록을 다루는 신뢰 기술에서는 이런 방식이 위험하다.
기록의 수집, 저장, 접근, 분석, 공개, 삭제는 서비스의 핵심 구조에 처음부터 포함되어야 한다.
본 문서의 신뢰 기록 최소화 원칙은 Privacy by Design과 같은 방향을 가진다.
믿집과 같은 서비스에서 개인정보 보호는 나중에 추가하는 옵션이 되어서는 안 된다. 초기 MVP 단계부터 다음 질문이 포함되어야 한다.
무엇을 수집하지 않을 것인가.
무엇을 저장하지 않을 것인가.
어떤 정보는 브라우저 안에서만 처리할 것인가.
어떤 정보는 익명·비식별 형태로만 다룰 것인가.
사용자가 결과를 직접 저장하거나 삭제할 수 있는가.
원본 정보 대신 판단값만 제공할 수 있는가.
민감 정보가 서버에 남지 않도록 할 수 있는가.
AI 기반 기능이 포함된다면 질문은 더 확장된다.
AI가 어떤 정보를 분석할 것인가.
AI가 어떤 원본 정보에 접근하지 않도록 할 것인가.
AI 판단의 근거와 한계를 어떻게 설명할 것인가.
AI가 생성한 결과를 최종 판단으로 오해하지 않도록 어떻게 안내할 것인가.

Privacy by Design은 본 문서에서 더 넓은 의미를 가진다.
본 문서에서는 이를 Trust by Design, 즉 신뢰 설계의 출발점으로 본다.
진정한 신뢰 기술은 나중에 보안을 붙이는 것이 아니라, 처음부터 기록의 위험을 알고 설계되어야 한다.
보호는 기능 뒤에 붙는 장식이 아니다.
보호는 신뢰 기술의 뼈대다.
10.4 선택적 공개와의 관계
선택적 공개는 원본 정보 전체를 공개하지 않고, 필요한 사실만 제한적으로 증명하거나 제공하는 방식을 의미한다.
이는 기록의 양면성 문제를 해결하기 위한 중요한 방향이다.
디지털 사회에서 신뢰를 만들기 위해 모든 정보를 공개하는 방식은 매우 위험하다.
예를 들어 어떤 사람이 특정 조건을 충족했는지 확인하기 위해 그 사람의 전체 신분 정보나 전체 생활 기록을 보여줄 필요는 없다.
필요한 것은 전체 공개가 아니라 특정 사실의 검증이다.
성인 여부를 확인할 때 필요한 것은 주민등록번호 전체가 아니라 성인 여부다.
계약 위험을 판단할 때 필요한 것은 계약서 원본 전체가 아니라 위험 조항이나 확인 필요 항목이다.
디지털 실존을 증명할 때 필요한 것은 인간의 모든 행위 기록이 아니라 특정 시점의 행위 진위다.
본 문서의 신뢰 기록 최소화 원칙은 선택적 공개와 직접적으로 연결된다.
본 문서는 선택적 공개를 단순한 개인정보 보호 기술이 아니라, 미래 신뢰 판단의 핵심 구조로 본다.
선택적 공개는 두 가지 가치를 동시에 달성한다.
첫째, 필요한 검증을 가능하게 한다.
둘째, 불필요한 노출을 줄인다.
믿집에서 선택적 공개는 이렇게 작동할 수 있다.
사용자의 계약서 원본을 공개하지 않아도 위험 신호 판단값을 제공할 수 있다.
정확한 주소를 저장하지 않아도 건물 유형이나 지역 수준의 위험 신호를 검토할 수 있다.
개인정보를 수집하지 않아도 사용자의 결과 이해도와 사용 의향을 테스트할 수 있다.
원본 계약 정보를 서버에 남기지 않아도 사용자가 직접 리포트를 내려받을 수 있다.

DET에서도 선택적 공개는 핵심이다.
디지털 실존을 증명한다는 이유로 모든 행위를 공개해서는 안 된다.
필요한 순간에 필요한 사실만 증명해야 한다.
AI 기반 신뢰 판단에서도 선택적 공개는 중요하다.
AI가 모든 원본 정보에 접근하는 것이 아니라, 필요한 신호만 제한적으로 분석하고 판단값을 제공하는 방향이 더 안전하다.
따라서 선택적 공개는 본 문서의 철학을 기술적으로 실현하는 가장 중요한 방향 중 하나다.
10.5 영지식 증명과의 관계
영지식 증명은 어떤 사실이 참이라는 것을 증명하면서도, 그 사실을 증명하는 데 사용된 원본 정보나 세부 내용을 공개하지 않는 암호학적 접근이다.
쉽게 말해, “내가 이 조건을 만족한다”는 사실을 보여주되, 그 조건을 만족하는 데 필요한 민감한 원본 정보는 드러내지 않는 방식이다.
이 개념은 본 문서의 관점과 매우 잘 맞는다.
본 문서가 말하는 핵심은 다음과 같다.
원본 정보를 모두 공개하지 않아도 신뢰는 만들 수 있어야 한다.
필요한 사실만 검증할 수 있어야 한다.
민감한 정보는 보호되어야 한다.
검증은 가능해야 하지만, 노출은 최소화되어야 한다.
이 방향은 영지식 증명의 철학과 연결된다.
다만 본 문서는 영지식 증명을 특정 기술 구현 방식으로 직접 한정하지 않는다.
본 문서는 암호학적 구현 이전의 상위 철학을 다룬다.
즉, 본 문서는 다음과 같은 질문을 던진다.
왜 원본 전체를 공개하지 않아야 하는가.
왜 필요한 사실만 증명하는 구조가 필요한가.
왜 디지털 실존과 신뢰 판단은 사생활 보호와 함께 설계되어야 하는가.
영지식 증명은 이 질문에 대한 하나의 기술적 응답이 될 수 있다.
믿집의 초기 단계에서 영지식 증명이 바로 적용될 필요는 없다.
하지만 장기적으로는 계약 위험 판단, 신원 확인, 디지털 실존 증명, 인증 행위 검증, 권한 확인 구조에서 영지식 증명과 유사한 방향의 기술이 중요해질 수 있다.
예를 들어 사용자는 특정 조건을 충족했음을 증명할 수 있지만, 자신의 전체 계약 정보나 신분 정보를 공개하지 않을 수 있다.

어떤 행위가 본인 승인에 의한 것임을 증명할 수 있지만, 전체 활동 기록을 공개하지 않을 수 있다.
본 문서는 이러한 방향을 철학적으로 지지한다.
미래의 신뢰 기술은 “더 많이 보여주는 기술”이 아니라, “덜 보여주고도 필요한 것을 증명하는 기술”이어야 한다.

10.6 DID와의 관계

DID, 즉 탈중앙화 신원 개념은 개인이 자신의 디지털 신원과 증명 정보를 보다 주체적으로 관리할 수 있도록 하는 방향과 관련된다.
기존의 신원 구조에서는 플랫폼, 기업, 기관이 사용자의 신원 정보를 보유하고 검증하는 경우가 많다. 이 구조는 편리하지만, 신원 정보가 특정 주체에게 집중될 수 있다는 위험을 가진다.
DID는 이러한 문제의식에서 출발한다.
개인이 자신의 신원 정보를 더 직접적으로 통제하고, 필요한 순간에 필요한 증명만 제시할 수 있는 방향을 제안한다.
본 문서의 관점은 DID와 연결된다.
기록은 사용자와 분리되어 존재해서는 안 된다.
사용자는 자신의 기록이 어떻게 쓰이는지 알고, 가능한 범위에서 통제할 수 있어야 한다.
신원과 행위의 증명은 필요하지만, 그것이 개인의 모든 정보를 플랫폼이나 기관에 맡기는 방식이어서는 안 된다.
DET 역시 DID와 연결될 수 있다.
DET가 디지털 실존 증명 구조라면, DID는 그 실존과 신원을 사용자가 주체적으로 관리할 수 있게 하는 기반 개념 중 하나가 될 수 있다.
그러나 본 문서는 DID를 그대로 수용하는 데 머물지 않는다.
본 문서는 DID보다 더 넓은 질문을 다룬다.
디지털 신원이 존재한다면, 그것은 무엇을 증명해야 하는가.
신원을 증명하기 위해 어느 정도의 기록이 필요한가.
사용자는 자신의 신원 기록을 어떻게 통제해야 하는가.
디지털 실존 증명은 감시로 변질되지 않을 수 있는가.
신원 증명과 사생활 보호는 어떻게 균형을 가져야 하는가.
DID는 이 질문에 대한 중요한 기술적·구조적 답변 중 하나다.
그러나 본 문서의 중심은 DID 자체가 아니라, 디지털 신원과 기록이 인간을 보호하는 방향으로 설계되어야 한다는 철학이다.
따라서 본 문서는 DID를 디지털 실존과 신뢰 기록 최소화 원칙을 구현할 수

있는 하위 기술·구조 개념으로 본다.
10.7 블록체인·감사 로그와의 관계
블록체인과 감사 로그는 기록의 무결성, 추적 가능성, 위변조 방지와 연결된다.
블록체인은 기록이 임의로 변경되기 어렵도록 분산 구조와 암호학적 연결을 활용하는 방식으로 이해될 수 있다. 감사 로그는 시스템 안에서 누가 언제 무엇을 했는지 추적할 수 있도록 남기는 기록이다.
이들은 기록의 신뢰성을 높이는 데 중요한 역할을 할 수 있다.
기록이 조작되면 신뢰는 무너진다.
누가 언제 어떤 정보를 변경했는지 알 수 없다면 책임을 묻기 어렵다.
접근과 변경 이력이 없다면 시스템 내부의 부정행위를 확인하기 어렵다.
따라서 블록체인과 감사 로그는 신뢰 기록의 중요한 기반이 될 수 있다.
그러나 본 문서는 여기서 한 가지 중요한 경고를 덧붙인다.
위변조 방지가 곧 안전을 의미하지는 않는다.
어떤 기록이 변조되지 않았다고 해서, 그 기록을 영구히 공개하거나 무제한 저장해도 된다는 뜻은 아니다.
오히려 민감한 정보가 잘못 기록되어 영구적으로 남을 경우, 그 불변성은 보호가 아니라 위험이 될 수 있다.
블록체인과 감사 로그는 기록의 진실성을 강화할 수 있지만, 동시에 기록 과잉과 삭제 불가능성의 문제를 만들 수 있다.
따라서 기록 기술은 무결성과 프라이버시를 함께 고려해야 한다.
좋은 기록 시스템은 다음의 균형을 가져야 한다.
조작되지 않아야 한다.
필요한 접근은 추적 가능해야 한다.
그러나 민감한 원본 정보는 무분별하게 공개되지 않아야 한다.
목적이 끝난 기록은 최소화되어야 한다.
사용자의 통제권과 사생활 보호가 고려되어야 한다.
본 문서의 관점에서 블록체인과 감사 로그는 신뢰 기술의 중요한 하위 요소다.
그러나 그것만으로 충분하지 않다.
기록을 안전하게 만든다는 것은 단순히 기록을 바꾸지 못하게 하는 것이 아니다.
기록을 안전하게 만든다는 것은 무엇을 기록할지, 어디까지 공개할지, 얼마나 보관할지, 누가 접근할지, 어떤 판단값으로 변환할지를 함께 설계하는 것이다.
10.8 AI 신뢰·AI 거버넌스와의 관계

본 문서는 AI 신뢰와 AI 거버넌스의 문제와도 연결된다.
AI 신뢰는 인공지능이 생성하거나 판단한 결과를 사람이 신뢰할 수 있는가의 문제다.
AI 거버넌스는 인공지능이 어떤 데이터로 작동하고, 어떤 기준으로 판단하며, 어떤 책임 구조 안에서 사용되어야 하는가의 문제다.
기록의 양면성 원리는 AI 시대에 더욱 중요해진다.
AI는 기록을 단순한 저장물이 아니라 판단 가능한 신호로 변환할 수 있다. 계약서, 거래 기록, 대화 내용, 접속 기록, 인증 기록, 행동 패턴을 분석해 위험 신호를 발견하고 사용자의 의사결정을 보조할 수 있다.
그러나 AI는 동시에 기록의 위험을 증폭시킬 수 있다.
AI는 기록을 바탕으로 개인의 성향과 취약점을 추론할 수 있다.
AI는 맥락이 부족한 기록을 과도하게 해석할 수 있다.
AI는 편향된 데이터에 기반해 부정확한 판단을 만들 수 있다.
AI는 실제처럼 보이는 허위 문서, 이미지, 음성, 영상, 대화 기록을 생성할 수 있다.
AI는 복잡한 판단을 그럴듯한 문장으로 포장해 사용자가 과도하게 신뢰하도록 만들 수 있다.
따라서 AI 기반 신뢰 기술은 반드시 기록의 양면성 원리 위에서 설계되어야 한다.
AI가 더 많은 데이터를 가질수록 더 신뢰할 수 있다는 생각은 위험하다.
AI가 더 많은 기록을 분석할수록 더 정확하다는 생각도 항상 맞지 않다.
중요한 것은 데이터의 양이 아니라, 어떤 기록을 어떤 목적과 권한으로 사용하고, 어떤 판단값으로 변환하며, 그 한계를 어떻게 설명하는가이다.
AI 기반 신뢰 기술에는 다음 원칙이 필요하다.
첫째, 필요한 기록만 사용해야 한다.
둘째, 민감한 원본 정보는 보호되어야 한다.
셋째, AI 판단은 설명 가능해야 한다.
넷째, AI 판단은 확정이 아니라 보조 신호로 제공되어야 한다.
다섯째, 사용자는 AI 판단의 근거와 한계를 이해할 수 있어야 한다.
여섯째, AI 생성물은 출처와 생성 여부가 검증 가능해야 한다.
일곱째, AI는 감시가 아니라 보호를 위해 사용되어야 한다.
본 문서는 AI를 단순한 자동화 도구로 보지 않는다.
AI는 기록을 신뢰로 바꿀 수 있는 도구이면서, 동시에 기록을 위험으로 증폭시킬 수 있는 도구다.

따라서 AI 시대의 신뢰 기술은 기록 최소화, 선택적 공개, 판단값 제공, 설명 가능성, 사용자 통제권, 생성물 출처 검증의 원칙 위에서 설계되어야 한다.

10.9 본 문서의 차별점: 흩어진 개념을 신뢰 판단 철학으로 재구성

본 문서의 차별점은 기존 개념들을 하나의 신뢰 판단 철학으로 재구성한다는 점에 있다.

프라이버시 보호, 데이터 최소화, Privacy by Design, 선택적 공개, 영지식 증명, DID, 블록체인, 감사 로그, AI 신뢰와 AI 거버넌스는 각각 중요한 개념이다. 그러나 이 개념들은 서로 다른 분야에서 별도로 논의되는 경우가 많다.

프라이버시는 권리의 언어로 설명된다.

데이터 최소화는 규제와 보호의 언어로 설명된다.

Privacy by Design은 시스템 설계의 언어로 설명된다.

선택적 공개와 영지식 증명은 암호학과 신원 증명의 언어로 설명된다.

DID는 디지털 신원과 주권의 언어로 설명된다.

블록체인과 감사 로그는 위변조 방지와 추적 가능성의 언어로 설명된다.

AI 신뢰와 AI 거버넌스는 자동화된 판단, 생성, 책임, 설명 가능성의 언어로 설명된다.

본 문서는 이 흩어진 언어들을 하나의 상위 질문 아래에 놓는다.

기록은 신뢰와 위험으로 어떻게 갈라지는가.

이 질문은 디지털 사회 전체를 관통한다.

기록은 신뢰를 만든다.

그러나 기록은 위험도 만든다.

기록은 증거가 된다.

그러나 기록은 감시가 될 수 있다.

기록은 피해자를 보호한다.

그러나 기록은 협박의 도구가 될 수 있다.

기록은 진실을 밝힌다.

그러나 기록은 조작된 진실을 만들 수 있다.

AI는 기록을 해석해 위험을 발견할 수 있다.

그러나 AI는 기록을 과도하게 추론하거나 허위 기록을 생성할 수도 있다.

따라서 본 문서는 단순한 개인정보 보호 문서가 아니다.

또한 단순한 보안 기술 문서도 아니다.

단순한 블록체인, DID, 영지식 증명 설명서도 아니다.

단순한 AI 신뢰나 AI 거버넌스 문서도 아니다.

본 문서는 기록의 양면성을 최상위 원리로 정의하고, 그 원리에서 신뢰 기록

최소화 원칙, 선택적 검증, 판단값 제공, 사용자 보호, AI 판단 보조, Trust Score, DET, 믿집의 서비스 철학을 파생시키는 원천 개념 문서다.
본 문서의 핵심 차별점은 다음과 같다.
첫째, 기록을 단순 저장물이 아니라 신뢰와 위험이 동시에 분화되는 문명적 힘으로 본다.
둘째, 신뢰를 정보의 양이 아니라 기록을 다루는 구조에서 나온다고 본다.
셋째, 프라이버시 보호를 신뢰 기술의 부가 기능이 아니라 기본 조건으로 본다.
넷째, 원본 정보의 공개보다 판단값 제공을 더 안전한 신뢰 방식으로 본다.
다섯째, 디지털 실존 증명을 감시가 아니라 선택적 검증과 보호의 구조로 해석한다.
여섯째, AI를 최종 판단자가 아니라 기록을 판단 가능한 신호로 변환하는 보조자로 본다.
일곱째, 믿집과 Trust Score를 단순 서비스 기능이 아니라 기록 기반 신뢰 판단 철학의 적용 사례로 본다.
여덟째, 미래 신뢰 기술의 방향을 “더 많이 기록하는 기술”이 아니라 “필요한 기록을 안전하게 증명하는 기술”로 정의한다.
이것이 본 문서의 가장 중요한 차별점이다.
기존 개념들은 각각의 영역에서 이미 존재한다.
그러나 본 문서는 그 개념들을 하나의 문명적 질문으로 묶는다.
좋은 디지털 사회는 무엇을 기록하고, 무엇을 보호하며, 무엇만 검증해야 하는가.
본 문서의 답은 다음과 같다.
좋은 디지털 사회는 모든 것을 기록하는 사회가 아니다.
좋은 디지털 사회는 필요한 기록을 안전하게 다루고, 필요한 사실만 검증하며, 인간이 스스로를 보호할 수 있도록 돕는 사회다.
이 지점에서 본 문서는 기존 개념들을 넘어, 기록 사회의 신뢰 판단 철학을 제안한다.

11. 적용 가능한 영역

기록의 양면성 원리와 신뢰 기록 최소화 원칙은 특정 산업 하나에만 적용되는 개념이 아니다.
이 원칙은 디지털 사회에서 기록이 생성되고, 저장되고, 해석되고, 검증되는

모든 영역에 적용될 수 있다.
기록은 계약, 금융, 행정, 의료, 법률, 창작, 신원, 거래, 상담, 인증 등 다양한 영역에서 신뢰의 근거가 된다. 그러나 동시에 기록은 사생활 침해, 감시, 유출, 조작, 협박, 범죄 악용의 위험도 만든다.
따라서 앞으로의 디지털 서비스와 신뢰 기술은 단순히 기록을 많이 남기는 방향이 아니라, 필요한 기록만 안전하게 구조화하고, 필요한 순간에만 검증 가능한 판단값을 제공하는 방향으로 설계되어야 한다.
본 장에서는 이 원칙이 적용될 수 있는 주요 영역을 정리한다.
11.1 부동산 계약 전 위험 판단
부동산 계약은 기록과 신뢰 판단이 가장 직접적으로 충돌하는 영역 중 하나다.
계약서, 등기부등본, 보증금, 실거래가, 소유자 정보, 권리관계, 특약, 중개 설명, 입금 내역 등 다양한 기록이 존재하지만, 일반 사용자가 이를 종합해 계약 위험을 판단하기는 어렵다.
부동산 계약에서 문제는 정보가 전혀 없다는 데만 있지 않다.
문제는 흩어진 정보가 위험 신호로 구조화되지 않는 데 있다.
따라서 부동산 계약 전 위험 판단에는 다음 원칙이 필요하다.
필요한 위험 신호만 수집한다.
민감한 계약 원본은 최소화한다.
사용자가 놓치기 쉬운 항목을 구조화한다.
원본 정보의 무분별한 저장보다 판단값 제공을 우선한다.
위험 신호를 Trust Score, PASS/HOLD/STOP과 같은 이해 가능한 형태로 제공한다.
부동산 계약 전 위험 판단에서 중요한 것은 “계약이 안전하다”고 단정하는 것이 아니다.
중요한 것은 사용자가 계약 전에 무엇을 확인해야 하는지 보이게 만드는 것이다.
믿집은 이 원칙이 적용될 수 있는 대표적 사례다.
11.2 전자계약과 계약서 검토
전자계약과 계약서 검토 영역에서도 기록의 양면성 원리는 중요하다.
전자계약은 계약의 편의성과 증거력을 높인다.
서명 시점, 당사자 정보, 동의 기록, 계약 조건, 수정 이력 등이 디지털 기록으로 남으면 분쟁 해결과 책임 확인에 도움이 된다.
그러나 계약서에는 민감한 정보가 포함된다.
이름, 주소, 금액, 계좌, 서명, 조건, 특약, 관계 정보가 포함될 수 있다. 이러

한 기록이 무분별하게 저장되거나 외부에 노출되면 큰 피해가 발생할 수 있다. 따라서 전자계약과 계약서 검토 시스템은 단순히 계약서를 저장하는 데 그쳐서는 안 된다.
계약서 원본은 보호되어야 하며, 사용자가 이해해야 할 위험 조항, 불리한 특약, 설명 불일치, 추가 확인 항목은 판단값으로 구조화되어야 한다.
AI는 계약서 검토를 도울 수 있다.
그러나 AI가 계약 안전을 보장하는 최종 판단자가 되어서는 안 된다. AI는 위험 문구를 찾고, 확인 필요 항목을 정리하고, 전문가 상담이 필요한 부분을 안내하는 보조 도구여야 한다.
계약서 검토의 미래는 원본을 많이 보관하는 방향이 아니라, 원본에서 필요한 위험 신호를 안전하게 추출하고 사용자에게 이해 가능한 형태로 제공하는 방향이어야 한다.
11.3 금융 거래와 대출 심사 보조
금융 거래와 대출 심사 영역은 기록 기반 판단이 매우 강하게 작동하는 영역이다.
소득, 신용, 부채, 거래 내역, 상환 이력, 자산 정보, 계좌 흐름 등 다양한 기록이 금융 판단의 근거가 된다. 이러한 기록은 금융기관이 위험을 판단하고, 사용자가 적절한 금융 서비스를 이용하는 데 도움이 된다.
그러나 금융 기록은 매우 민감하다.
경제 상태는 개인의 취약성과 직결된다.
금융 기록이 외부에 노출되면 사기, 협박, 차별, 불리한 평가, 심리적 부담으로 이어질 수 있다.
따라서 금융 영역에서도 신뢰 기록 최소화 원칙이 필요하다.
모든 금융 기록을 무분별하게 보여주는 방식이 아니라, 특정 판단에 필요한 신호만 구조화해야 한다. 대출 심사 보조나 금융 위험 안내 서비스는 원본 금융 정보 전체를 드러내기보다, 상환 부담, 고정비 압박, 연체 위험, 현금흐름 안정성 같은 판단값을 제공하는 방향이 더 안전하다.
AI가 금융 기록을 분석할 경우에는 더욱 신중해야 한다.
AI는 개인의 금융 취약성을 추론할 수 있기 때문에, 판단 기준과 한계, 사용 목적, 접근 권한이 명확해야 한다.
금융 신뢰는 데이터의 양이 아니라, 데이터를 어떻게 보호하면서 판단하는가에서 나온다.
11.4 보험·보증 심사
보험과 보증 심사는 위험 판단을 기반으로 한다.

보험사는 사고 가능성, 건강 상태, 재산 상태, 계약 이력, 청구 이력 등을 판단하고, 보증기관은 보증 가능성, 상환 가능성, 담보 위험, 계약 위험 등을 평가한다.
이 과정에서 많은 기록이 필요할 수 있다.
그러나 보험·보증 영역의 기록은 민감성이 높다.
건강 정보, 재산 정보, 가족 관계, 직업 정보, 금융 상태, 계약 조건이 포함될 수 있다.
따라서 보험·보증 심사에서도 기록의 양면성을 고려해야 한다.
위험 판단은 필요하지만, 판단을 위해 필요한 범위를 넘어 개인의 삶 전체를 들여다보는 구조가 되어서는 안 된다.
보험·보증 심사의 미래는 다음 방향을 가져야 한다.
필요한 위험 신호만 검토한다.
민감 원본은 제한적으로 보호한다.
사용자에게 판단 기준과 한계를 설명한다.
불필요한 장기 보관과 목적 외 사용을 제한한다.
가능하다면 원본 공개보다 검증 가능한 상태값과 판단값을 활용한다.
보험과 보증의 신뢰는 위험을 계산하는 능력뿐 아니라, 사람의 민감한 기록을 안전하게 다루는 능력에서 나온다.
11.5 중고거래와 사기 예방
중고거래는 개인 간 신뢰가 중요한 영역이다.
판매자와 구매자는 서로를 잘 모르는 상태에서 거래한다. 이때 거래 기록, 계정 이력, 후기, 인증 여부, 결제 기록, 배송 정보 등이 신뢰 판단의 근거가 된다.
그러나 중고거래에서도 기록은 양면성을 가진다.
거래 기록과 후기 시스템은 사기를 줄일 수 있다.
그러나 지나친 개인정보 공개는 스토킹, 협박, 신원 노출, 사기 표적화로 이어질 수 있다.
중고거래에서 필요한 것은 상대방의 모든 개인정보가 아니다.
필요한 것은 거래 안전에 필요한 신뢰 신호다.
예를 들어 다음과 같은 판단값이 중요할 수 있다.
계정 생성 이후 거래 이력.
최근 이상 거래 패턴.
반복 신고 여부.
입금 방식 위험 신호.

외부 링크 유도 여부.
급한 거래 압박 신호.
가격이 비정상적으로 낮은지 여부.
이러한 신호는 원본 개인정보 전체를 공개하지 않고도 거래 위험을 줄일 수 있다.
AI는 중고거래 사기 패턴을 탐지하는 데 도움을 줄 수 있다.
그러나 AI가 사용자 전체의 사적 거래 기록을 과도하게 분석하거나, 사람을 부당하게 분류하는 구조가 되어서는 안 된다.
중고거래의 신뢰 기술 역시 “더 많이 공개하는 구조”가 아니라 “필요한 신호만 안전하게 보여주는 구조”로 가야 한다.
11.6 보이스피싱 위험 신호 판단
보이스피싱과 금융 사기는 기록과 신호 분석이 중요한 영역이다.
보이스피싱은 단일 행위로 발생하지 않는다.
대화 패턴, 송금 요구, 긴급한 압박, 기관 사칭, 링크 클릭 유도, 앱 설치 요구, 개인정보 요구, 가족·지인 사칭 등 여러 신호가 결합되어 발생한다.
이때 기록은 피해 예방에 도움이 될 수 있다.
사용자가 받은 메시지, 통화 내용의 일부, 요구된 행동, 송금 요청 방식, 상대방의 말투와 압박 정도는 위험 판단의 신호가 될 수 있다.
그러나 보이스피싱 예방을 위해 사용자의 모든 대화나 통화 기록을 저장하는 방식은 위험하다.
필요한 것은 전체 대화의 저장이 아니라 위험 신호의 구조화다.
예를 들어 다음과 같은 판단값이 제공될 수 있다.
기관 사칭 가능성.
긴급 압박 신호.
송금 유도 신호.
앱 설치 요구 신호.
개인정보 요구 신호.
대화 중단 및 공식 기관 확인 권고.
AI는 이러한 위험 신호를 분석하는 데 강력한 도구가 될 수 있다.
하지만 AI가 사용자의 사적 대화 전체를 무제한 저장하고 분석하는 방식은 신중해야 한다.
보이스피싱 예방에서 기록은 감시가 아니라 보호를 위해 사용되어야 한다.
사용자의 사적인 대화를 수집하는 것이 아니라, 위험 신호를 사용자가 이해할 수 있게 변환하는 것이 핵심이다.

11.7 공공 행정과 민원 기록

공공 행정과 민원 영역에서도 기록은 필수적이다.

민원 접수, 처리 과정, 담당자 응답, 행정 결정, 승인과 거절, 보완 요청, 처리 기간은 모두 기록으로 남아야 한다. 이러한 기록은 행정의 투명성과 책임성을 높인다.

기록이 없다면 행정은 불투명해지고, 민원인은 자신의 권리를 주장하기 어렵다.

그러나 공공 행정 기록에도 위험이 있다.

민원 기록에는 개인의 주소, 가족관계, 건강, 경제적 상황, 분쟁 내용, 피해 사실, 민감한 사정이 포함될 수 있다. 이러한 기록이 부적절하게 공개되면 민원인에게 2차 피해가 발생할 수 있다.

따라서 공공 행정 기록은 책임성과 보호를 동시에 가져야 한다.

행정기관은 필요한 처리 기록을 남겨야 한다.

그러나 민원인의 민감 정보는 보호해야 한다.

공개가 필요한 경우에도 비식별화와 목적 제한이 필요하다.

기록은 행정의 책임을 위한 것이지, 민원인의 삶을 노출하기 위한 것이 아니다.

AI가 행정 기록을 분석할 경우에도 이 원칙은 유지되어야 한다.

AI는 민원 분류와 처리 효율을 높일 수 있지만, 민원인을 감시하거나 취약성을 부당하게 평가하는 방식으로 사용되어서는 안 된다.

공공 영역에서 좋은 기록 체계는 투명성과 사생활 보호를 함께 설계하는 체계다.

11.8 의료·상담·법률 기록 보호

의료, 상담, 법률 기록은 가장 민감한 기록에 속한다.

의료 기록은 개인의 건강과 질병, 치료, 약물, 정신 상태를 포함할 수 있다.

상담 기록은 개인의 감정, 가족 관계, 상처, 불안, 과거 경험을 포함할 수 있다.

법률 기록은 분쟁, 피해, 범죄, 계약, 재산, 가족 문제와 연결될 수 있다.

이 기록들은 개인을 보호하기 위해 필요하다.

의사는 진료 기록이 있어야 치료를 이어갈 수 있고, 상담자는 상담 맥락을 이해해야 하며, 변호사는 사건 기록을 바탕으로 법률 조력을 제공한다.

그러나 이 기록들이 유출되면 피해는 매우 크다.

의료·상담·법률 기록은 단순 정보가 아니다.

그것은 인간의 가장 취약한 순간을 담은 기록이다.

따라서 이 영역에서는 신뢰 기록 최소화 원칙이 더욱 강하게 적용되어야 한다.
필요한 전문가만 접근해야 한다.
원본 기록은 강하게 보호되어야 한다.
목적 외 사용은 제한되어야 한다.
사용자는 자신의 기록이 어떻게 쓰이는지 알 수 있어야 한다.
불필요한 공개는 금지되어야 한다.
가능하다면 원본이 아니라 필요한 판단값과 요약 정보만 제한적으로 활용해야 한다.
AI가 의료·상담·법률 기록을 분석할 경우에는 특히 조심해야 한다.
AI는 보조 도구가 될 수 있지만, 인간의 고통과 복잡한 맥락을 단순한 분류값으로 환원해서는 안 된다.
의료·상담·법률 기록은 인간을 평가하기 위한 기록이 아니라, 인간을 보호하기 위한 기록이어야 한다.
11.9 AI 생성물·AI 판단·출처 검증
AI 생성물과 AI 판단은 기록의 양면성 원리가 강하게 적용되는 영역이다.
AI는 문서, 이미지, 영상, 음성, 코드, 음악, 대화, 보고서 등 다양한 결과물을 생성할 수 있다. 이러한 생성 능력은 창작과 생산성을 높일 수 있지만, 동시에 허위 기록과 조작 콘텐츠의 위험을 키운다.
앞으로 중요한 질문은 다음과 같다.
이 콘텐츠는 사람이 만든 것인가, AI가 만든 것인가.
이 기록은 실제 행위의 흔적인가, 생성된 허위 기록인가.
이 음성은 실제 발화인가, 합성된 음성인가.
이 영상은 실제 장면인가, 조작된 영상인가.
이 문서는 원본인가, AI가 재구성한 문서인가.
이 판단은 사람이 내린 것인가, AI가 보조한 것인가.
AI 판단의 근거는 무엇인가.
AI 판단의 한계는 무엇인가.
AI 시대에는 기록의 출처 검증이 더욱 중요해진다.
기록이 실제인지, 조작되었는지, AI가 생성했는지, 인간이 승인했는지 확인할 수 있어야 한다. 그러나 이를 위해 창작자나 사용자의 모든 사생활과 작업 과정을 공개할 필요는 없다.
필요한 것은 출처와 생성 여부, 변경 여부, 승인 여부에 대한 검증 가능한 기록이다.
AI 판단 역시 마찬가지다.

AI가 계약서 위험 신호를 분석하거나, 거래 위험을 평가하거나, 보이스피싱 가능성을 탐지하거나, 신뢰 점수를 보조할 수 있다. 그러나 AI 판단은 절대적 결론이 아니라 판단 보조 신호로 제공되어야 한다.
AI 판단에는 근거와 한계가 함께 제시되어야 한다.
어떤 기록을 바탕으로 판단했는지.
어떤 위험 신호가 반영되었는지.
어떤 정보가 부족한지.
어떤 부분은 전문가 확인이 필요한지.
AI가 확정할 수 없는 영역은 무엇인지.
이러한 설명이 없다면 AI 판단은 신뢰 기술이 아니라 불투명한 권력이 될 수 있다.
따라서 AI 생성물과 AI 판단의 미래는 다음 원칙을 가져야 한다.
생성물의 출처를 검증할 수 있어야 한다.
AI 생성 여부를 확인할 수 있어야 한다.
AI 판단의 근거를 설명할 수 있어야 한다.
민감한 원본 정보는 보호되어야 한다.
사용자는 AI 판단을 최종 결론이 아니라 보조 신호로 이해해야 한다.
AI는 감시와 조작이 아니라 보호와 검증을 위해 사용되어야 한다.
AI 시대의 신뢰 기술은 더 많은 기록을 소유하는 기술이 아니라, 기록의 출처와 판단 근거를 안전하게 검증하는 기술이어야 한다.
11.10 디지털 신원과 행위 증명
디지털 신원과 행위 증명은 기록의 양면성이 가장 강하게 드러나는 영역이다.
디지털 사회에서는 누가 실제 사람인지, 누가 어떤 권한을 가졌는지, 누가 어떤 행위를 했는지, 그 행위가 실제 본인의 의사였는지 증명해야 하는 순간이 많아진다.
전자계약, 금융 거래, 행정 서비스, 의료 서비스, 창작물 등록, 플랫폼 활동, 투표, 인증, 결제 등에서 디지털 신원과 행위 증명은 중요해질 수밖에 없다.
그러나 신원 증명은 항상 사생활 침해의 위험을 가진다.
신원을 증명한다는 이유로 사용자의 모든 기록을 공개해서는 안 된다.
행위를 증명한다는 이유로 사용자의 전체 활동 내역을 보여줘서는 안 된다.
필요한 것은 선택적 증명이다.
특정 시점에 특정 사용자가 특정 행위를 했는지 확인하면 된다.
그 사용자의 전체 삶을 공개할 필요는 없다.
DET는 이 영역과 직접적으로 연결된다.

DET는 디지털 실존과 행위의 진위를 증명하되, 사생활 전체를 노출하지 않는 방향으로 설계되어야 한다.
디지털 신원과 행위 증명의 미래는 감시가 아니라 신뢰의 기반이어야 한다.
그 신뢰는 필요한 사실만 안전하게 증명하는 구조에서 나와야 한다.

12. 본 문서의 지위와 한계

본 문서는 기록의 양면성 원리와 신뢰 기록 최소화 원칙을 정의한 원천 개념 문서이다.
이 문서는 특정 서비스의 기능 설명서도 아니고, 특정 기술의 구현 명세서도 아니다.
이 문서는 디지털 사회에서 기록이 신뢰와 위험으로 분화되는 구조를 설명하고, 미래 신뢰 기술이 어떤 철학적 방향 위에서 설계되어야 하는지를 정의한다.
본 문서는 믿집, DET, Trust Score와 같은 하위 개념의 상위 철학 기반으로 활용될 수 있다.
그러나 본 문서 자체가 세부 알고리즘이나 기술 구현 방식을 공개하는 것은 아니다.
본 장에서는 본 문서의 지위와 한계를 명확히 한다.
12.1 본 문서는 기술 구현 명세서가 아니다
본 문서는 기술 구현 명세서가 아니다.
본 문서는 특정 시스템을 어떻게 개발해야 하는지, 어떤 서버 구조를 가져야 하는지, 어떤 데이터베이스를 사용해야 하는지, 어떤 암호화 방식이나 인증 방식을 적용해야 하는지 상세히 설명하지 않는다.
또한 본 문서는 특정 서비스의 화면 구성, API 구조, 데이터 흐름, 내부 처리 방식, 보안 아키텍처를 구체적으로 공개하지 않는다.
본 문서의 목적은 구현보다 상위에 있다.
본 문서는 “어떤 기술을 만들 것인가”보다 먼저, “그 기술이 어떤 철학과 원칙 위에 있어야 하는가”를 정의한다.
기술은 철학 없이도 구현될 수 있다.
그러나 철학 없는 신뢰 기술은 인간을 보호하지 못하고, 오히려 감시와 통제의 도구가 될 수 있다.
따라서 본 문서는 구현의 설명서가 아니라 구현이 따라야 할 방향을 제시하는 문서다.

12.2 본 문서는 알고리즘 산식이나 가중치를 공개하지 않는다
본 문서는 알고리즘 산식이나 가중치를 공개하지 않는다.
Trust Score, PASS/HOLD/STOP, 위험 신호 구조화와 같은 표현은 본 문서에서 철학적·개념적 의미로 다루어진다.
이 문서는 해당 판단값이 어떤 세부 산식으로 계산되는지, 각 변수에 어떤 가중치가 부여되는지, 어떤 임계값에서 어떤 결과가 나오는지 공개하지 않는다.
그 이유는 명확하다.
첫째, 본 문서는 공개 아카이브용 원천 철학 문서이기 때문이다.
둘째, 세부 알고리즘과 가중치는 별도 기술 문서, 특허 문서, 영업비밀, 내부 설계 문서로 관리되어야 하기 때문이다.
셋째, 본 문서의 목적은 기술 구현을 노출하는 것이 아니라, 신뢰 기술의 상위 원칙을 정리하는 데 있기 때문이다.
따라서 본 문서에서 다루는 것은 “어떤 수식으로 계산하는가”가 아니다.
본 문서가 다루는 것은 다음 질문이다.
왜 위험 신호를 구조화해야 하는가.
왜 원본 정보보다 판단값이 중요할 수 있는가.
왜 기록은 최소화되어야 하는가.
왜 판단값은 사용자 보호를 위한 보조 신호여야 하는가.
왜 AI 판단은 확정이 아니라 보조 기능이어야 하는가.
세부 산식과 가중치는 본 문서의 범위를 벗어난다.
12.3 본 문서는 기록과 신뢰 기술의 철학적 방향을 정의한다
본 문서의 중심 목적은 기록과 신뢰 기술의 철학적 방향을 정의하는 것이다.
디지털 사회에서 기록은 계속 증가한다.
계약, 거래, 인증, 창작, 접속, 대화, 판단의 흔적은 점점 더 많은 데이터로 남는다.
그러나 기록의 증가는 자동으로 신뢰를 만들지 않는다.
기록은 신뢰를 만들 수 있지만, 위험도 만들 수 있다.
따라서 필요한 것은 기록을 바라보는 철학이다.
본 문서는 기록을 단순 데이터가 아니라 문명적 힘으로 본다.
기록은 문명의 기억이지만, 권한 없는 기록은 폭력이 될 수 있다.
기록은 악을 막는 도구이지만, 악을 조직하는 도구가 될 수도 있다.
인공지능 시대에는 이 문제가 더 커진다.
AI는 기록을 해석하고, 추론하고, 판단값으로 변환할 수 있지만, 동시에 허위 기록을 생성하고, 사생활을 과도하게 추론하며, 불투명한 판단을 만들 수도 있

다.
이 관점에서 본 문서는 미래 신뢰 기술의 방향을 다음과 같이 정의한다.
더 많이 저장하는 기술이 아니라, 필요한 기록을 안전하게 다루는 기술.
원본 정보를 무분별하게 공개하는 기술이 아니라, 필요한 사실만 검증하는 기술.
사용자를 감시하는 기술이 아니라, 사용자를 보호하는 기술.
불확실성을 숨기는 기술이 아니라, 위험 신호를 보이게 하는 기술.
AI를 최종 판단자로 세우는 기술이 아니라, AI를 설명 가능한 판단 보조자로 사용하는 기술.
이것이 본 문서가 정의하는 철학적 방향이다.
12.4 본 문서는 믿집·DET·Trust Score의 상위 개념 기반으로 활용될 수 있다
본 문서는 믿집, DET, Trust Score의 상위 개념 기반으로 활용될 수 있다.
믿집은 부동산 계약 전 위험 신호를 구조화하고, 사용자가 계약 전 놓치기 쉬운 위험을 판단하도록 돕는 서비스로 확장될 수 있다. 이때 믿집은 사용자의 모든 계약 정보를 저장하는 서비스가 아니라, 필요한 위험 신호만 최소화하여 판단값으로 제공하는 보호형 신뢰 서비스여야 한다.
Trust Score는 흩어진 위험 신호를 사용자가 이해 가능한 판단값으로 변환하는 개념이다. 이는 원본 정보를 무분별하게 공개하지 않고도 사용자가 현재 상태를 이해할 수 있도록 돕는 구조와 연결된다.
DET는 디지털 실존과 행위의 진위를 증명하되, 개인의 모든 행위와 사생활을 노출하지 않는 방향으로 설계되어야 한다. 이는 선택적 검증과 신뢰 기록 최소화 원칙의 직접적인 적용 영역이다.
AI 신뢰 판단 보조는 기록을 판단 가능한 신호로 변환하는 역할을 할 수 있다. 그러나 AI는 최종 판단자가 아니라, 위험 신호를 정리하고 근거를 설명하는 보조 도구로 활용되어야 한다.
따라서 본 문서는 이 네 가지 개념의 상위 철학적 기반이 될 수 있다.
기록의 양면성 원리에서 믿집은 계약 위험 판단으로 파생된다.
기록의 양면성 원리에서 Trust Score는 판단값 제공 구조로 파생된다.
기록의 양면성 원리에서 DET는 디지털 실존의 선택적 검증 구조로 파생된다.
기록의 양면성 원리에서 AI 신뢰 판단 보조는 기록 해석과 판단 근거 제공 구조로 파생된다.
이 문서는 각 개념의 세부 구현을 설명하지 않는다.
그러나 각 개념이 어떤 철학적 방향 위에서 설계되어야 하는지를 제시한다.
12.5 향후 별도 기술 문서, 특허 문서, 서비스 정책 문서로 확장 가능하다

본 문서는 향후 여러 문서로 확장될 수 있다.
첫째, 별도 기술 문서로 확장될 수 있다.
기록 최소화 구조, 판단값 생성 구조, 데이터 처리 방식, 보안 설계, 사용자 통제권 설계, 선택적 검증 구조, AI 판단 보조 구조 등을 기술 문서로 구체화할 수 있다.
둘째, 특허 문서로 확장될 수 있다.
위험 신호 구조화 방식, 판단값 생성 방식, Trust Score 산출 구조, DET 기반 검증 구조, AI 기반 위험 신호 분류 구조, 기록 최소화 기반 신뢰 판단 방식 등은 별도의 특허 검토 대상이 될 수 있다. 단, 본 문서에서는 이러한 구현 방식을 공개하지 않는다.
셋째, 서비스 정책 문서로 확장될 수 있다.
개인정보 처리 원칙, 데이터 저장 정책, 사용자 동의 정책, 리포트 생성과 삭제 정책, 민감정보 보호 원칙, AI 판단 고지, 책임 한계 고지 등이 정책 문서로 발전할 수 있다.
넷째, 윤리 원칙 문서로 확장될 수 있다.
기록은 감시가 아니라 보호를 위해 존재해야 한다는 원칙은 향후 신뢰 기술 윤리의 기준이 될 수 있다.
다섯째, 사업계획서와 브랜드 철학 문서로 확장될 수 있다.
믿집, DET, Trust Score, AI 신뢰 판단 보조가 단순 기술이 아니라 사용자 보호와 디지털 신뢰 철학 위에 서 있다는 점을 설명하는 기반 문서가 될 수 있다.
본 문서는 끝이 아니라 시작이다.
이 문서는 구체 기술을 모두 설명하지 않지만, 앞으로 어떤 기술과 서비스가 만들어져야 하는지 방향을 제시한다.

13. 최초 주장 요약

본 장은 앞선 내용을 압축하여 본 문서의 최초 주장을 정리한다.
이 문서의 핵심은 단순하다.
디지털 사회에서 기록은 계속 증가한다.
그러나 기록은 신뢰만 만드는 것이 아니다.
기록은 위험도 만든다.
인공지능은 이 구조를 더욱 강화한다.
AI는 기록을 분석해 신뢰 판단을 도울 수 있지만, 동시에 기록을 과도하게 추

론하고, 허위 기록을 생성하며, 불투명한 판단을 만들 수도 있다.
따라서 미래 신뢰 기술은 더 많이 기록하는 방향이 아니라, 필요한 기록만 안전하게 다루고, 필요한 사실만 검증하는 방향으로 가야 한다.
13.1 기록은 문명의 기억이지만 권한 없는 기록은 폭력이 된다
기록은 문명의 기억이다.
기록은 계약을 기억하고, 거래를 기억하고, 행위를 기억하고, 책임을 기억한다.
기록이 있기 때문에 사회는 말과 기억에만 의존하지 않고 근거를 통해 판단할 수 있다.
그러나 권한 없는 기록은 폭력이 된다.
동의 없이 수집된 기록, 목적 없이 저장된 기록, 권한 없이 공개된 기록, 맥락 없이 유포된 기록은 인간을 보호하지 않는다. 오히려 인간을 노출시키고, 공격하고, 통제할 수 있다.
따라서 기록은 반드시 권한과 목적, 보호 구조 안에서 다루어져야 한다.
기록은 존재 자체로 정당화되지 않는다.
기록은 정당한 목적과 안전한 구조 안에서만 신뢰가 된다.
13.2 기록은 악을 막는 도구이면서 악을 조직하는 도구가 될 수 있다
기록은 악을 막는 도구가 될 수 있다.
기록은 사기와 조작을 추적하고, 계약 위반을 확인하며, 책임 회피를 줄이고, 피해자가 억울함을 증명하도록 돕는다.
그러나 기록은 악을 조직하는 도구가 될 수도 있다.
악의적인 주체는 기록을 모아 타인의 약점을 찾고, 생활 패턴을 분석하고, 사생활을 협박의 수단으로 사용하며, 더 정교한 범죄를 계획할 수 있다.
AI는 이 위험을 더 크게 만들 수 있다.
AI는 기록을 분석해 개인의 취약점을 추론하고, 맞춤형 사기나 조작된 설득을 생성하며, 실제처럼 보이는 허위 기록을 만들 수 있다.
따라서 기록의 문제는 단순히 기록할 것인가, 하지 않을 것인가가 아니다.
핵심은 기록이 누구의 손에 있고, 어떤 권한으로 사용되며, 어떤 보호 구조 안에서 다루어지는가이다.
기록은 방패가 될 수 있다.
그러나 통제되지 않으면 칼이 된다.
13.3 미래 신뢰 기술은 더 많이 저장하는 기술이 아니라 필요한 것을 안전하게 증명하는 기술이어야 한다
미래 신뢰 기술의 방향은 무한 저장이 아니다.
모든 정보를 저장하는 시스템은 강력해 보일 수 있다.

그러나 모든 것을 저장하는 시스템은 모든 것이 유출될 수 있는 시스템이기도 하다.
미래 신뢰 기술은 필요한 사실을 필요한 순간에 안전하게 검증할 수 있어야 한다.
원본 정보 전체를 공개하지 않고도 필요한 판단을 제공할 수 있어야 한다.
개인의 모든 행위를 노출하지 않고도 특정 행위의 진위를 증명할 수 있어야 한다.
계약서 원본을 무분별하게 저장하지 않고도 위험 신호를 구조화할 수 있어야 한다.
AI가 기록을 분석하더라도, 그 분석은 필요한 범위 안에서 이루어져야 한다.
AI 판단은 확정이 아니라 보조 신호여야 하며, 그 근거와 한계가 설명되어야 한다.
더 많이 저장하는 기술이 아니라, 덜 노출하고도 필요한 것을 증명하는 기술이 미래의 신뢰 기술이어야 한다.
13.4 신뢰는 정보의 양이 아니라 기록을 다루는 구조에서 나온다
신뢰는 정보의 양에서 나오지 않는다.
많은 정보를 가진 시스템이 반드시 신뢰받는 것은 아니다.
오히려 많은 정보를 가진 시스템은 더 큰 유출 위험과 더 큰 감시 위험을 만들 수 있다.
신뢰는 기록을 다루는 구조에서 나온다.
무엇을 수집하는가.
무엇을 수집하지 않는가.
무엇을 저장하는가.
무엇을 저장하지 않는가.
누가 접근할 수 있는가.
사용자는 통제할 수 있는가.
원본을 공개하는가, 판단값을 제공하는가.
목적이 끝난 기록은 어떻게 처리되는가.
AI 판단은 어떤 근거로 생성되고, 그 한계는 어떻게 설명되는가.
이 질문에 대한 구조가 신뢰를 만든다.
따라서 미래의 신뢰 기술은 정보의 양을 자랑해서는 안 된다.
미래의 신뢰 기술은 기록을 안전하게 다루는 구조를 증명해야 한다.
13.5 믿집과 DET는 이 원칙 위에서 보호형 신뢰 기술로 설계되어야 한다
믿집과 DET는 기록의 양면성 원리와 신뢰 기록 최소화 원칙 위에서 설계되어

야 한다.
믿집은 사용자의 모든 계약 정보를 저장하는 서비스가 아니다.
믿집은 계약 전 위험 판단에 필요한 최소 신호를 구조화하고, Trust Score와 PASS/HOLD/STOP 판단값을 제공해 사용자가 스스로를 보호하도록 돕는 서비스여야 한다.
DET는 인간의 모든 디지털 행위를 공개하는 기술이 아니다.
DET는 필요한 순간에 필요한 사실만 증명하고, 디지털 실존과 행위의 진위를 확인하되, 개인의 원본 사생활을 보호하는 구조여야 한다.
AI 신뢰 판단 보조는 이 두 구조를 도울 수 있다.
그러나 AI는 최종 판단자가 아니라, 기록을 분석해 위험 신호를 정리하고 사용자가 이해할 수 있도록 돕는 보조자여야 한다.
이 개념들은 모두 같은 원칙 위에 서 있다.
기록은 감시가 아니라 보호를 위해 존재해야 한다.
신뢰는 노출이 아니라 안전한 검증에서 나와야 한다.
판단은 확정이 아니라 위험 신호의 구조화여야 한다.
AI는 통제가 아니라 보호를 위해 사용되어야 한다.
믿집과 DET는 보호형 신뢰 기술이어야 한다.

14. 최종 선언

본 문서의 최종 선언은 기록의 시대를 살아가는 디지털 사회에 대한 철학적 기준이다.
기술은 앞으로 더 많은 것을 기록할 것이다.
문명은 더 많은 행위를 데이터로 남길 것이다.
AI, 플랫폼, 전자계약, 디지털 신원, 공공데이터, 인증 시스템은 인간의 행동과 선택을 더 촘촘하게 기록할 것이다.
그러나 기록의 증가가 곧 문명의 성숙을 의미하지는 않는다.
기록이 인간을 보호하지 못한다면, 기록은 발전이 아니라 위험이 된다.
기록이 신뢰를 만들지 못하고 감시와 협박, 조작과 범죄 모의의 도구가 된다면, 그 기록은 문명의 기억이 아니라 문명의 상처가 된다.
따라서 좋은 디지털 문명은 기록의 양이 아니라 기록을 다루는 방식으로 평가되어야 한다.
14.1 좋은 문명은 많이 기록하는 문명이 아니다

좋은 문명은 많이 기록하는 문명이 아니다.
많이 기록한다는 것은 많은 증거를 남긴다는 뜻일 수 있다.
그러나 동시에 많은 위험을 저장한다는 뜻이기도 하다.
모든 행위가 기록되고, 모든 말이 저장되고, 모든 실수가 남고, 모든 관계가 데이터화되는 사회는 완벽해 보일 수 있다.
그러나 그런 사회에서 인간은 자유롭기 어렵다.
좋은 문명은 모든 것을 기억하는 문명이 아니다.
좋은 문명은 무엇을 기억해야 하고, 무엇을 보호해야 하며, 무엇을 잊을 수 있어야 하는지 아는 문명이다.
기록은 필요하다.
그러나 모든 기록이 필요한 것은 아니다.
문명은 기록의 양으로 성숙해지는 것이 아니라, 기록을 다루는 지혜로 성숙해진다.
14.2 좋은 문명은 필요한 기록을 안전하게 다루는 문명이다
좋은 문명은 필요한 기록을 안전하게 다루는 문명이다.
계약의 책임은 남겨야 한다.
거래의 근거는 남겨야 한다.
동의와 승인, 권한과 변경 이력은 필요한 경우 남겨야 한다.
피해자가 자신을 보호할 수 있는 기록은 남겨야 한다.
그러나 그 기록은 안전해야 한다.
권한 없는 사람에게 공개되어서는 안 된다.
목적 없이 저장되어서는 안 된다.
불필요하게 연결되어서는 안 된다.
맥락 없이 유통되어서는 안 된다.
인간을 협박하거나 감시하는 도구가 되어서는 안 된다.
필요한 기록을 남기되, 필요한 범위 안에서 다루어야 한다.
기록은 보호 구조와 함께 존재해야 한다.
AI가 기록을 분석하는 경우에도 이 원칙은 변하지 않는다.
AI가 더 많은 기록을 해석할 수 있다는 이유로 모든 기록이 AI에게 제공되어서는 안 된다. AI는 필요한 신호만 안전하게 해석하고, 그 판단의 근거와 한계를 설명해야 한다.
이것이 좋은 디지털 문명의 조건이다.
14.3 기록은 감시가 아니라 보호를 위해 존재해야 한다
기록은 감시가 아니라 보호를 위해 존재해야 한다.

감시를 위한 기록은 인간을 대상으로 본다.
보호를 위한 기록은 인간을 주체로 본다.
감시를 위한 기록은 더 많이 보려고 한다.
보호를 위한 기록은 필요한 것만 보려고 한다.
감시를 위한 기록은 권력이 소유한다.
보호를 위한 기록은 사용자가 의미와 범위를 이해하고 통제할 수 있어야 한다.
기록은 사람을 침묵하게 만들기 위해 존재해서는 안 된다.
기록은 사람을 두렵게 만들기 위해 존재해서는 안 된다.
기록은 인간의 삶을 영원히 과거에 묶어두기 위해 존재해서는 안 된다.
AI 역시 감시를 위해 사용되어서는 안 된다.
AI는 사람을 분류하고 통제하는 최종 판단자가 아니라, 위험 신호를 발견하고 사용자가 더 안전하게 판단하도록 돕는 보조 도구여야 한다.
기록은 사람이 위험을 피하고, 억울함을 줄이며, 스스로를 보호하기 위해 존재해야 한다.
이 원칙을 잃는 순간, 신뢰 기술은 감시 기술로 변질된다.
14.4 신뢰 기술의 미래는 기록의 소유가 아니라 기록의 안전한 검증에 있다
신뢰 기술의 미래는 기록의 소유가 아니라 기록의 안전한 검증에 있다.
누가 더 많은 데이터를 가지고 있는가가 중요한 시대에서, 누가 필요한 사실을 더 안전하게 증명할 수 있는가가 중요한 시대로 이동해야 한다.
미래의 신뢰 기술은 사용자의 모든 정보를 소유하려 해서는 안 된다.
미래의 신뢰 기술은 사용자가 필요한 순간에 필요한 사실만 증명할 수 있도록 도와야 한다.
특히 인공지능 시대에는 기록의 수집보다 기록의 해석이 더 큰 권력이 될 수 있다.
AI는 사람이 남긴 기록을 분석하고, 요약하고, 예측하고, 판단값으로 변환할 수 있다. 동시에 AI는 기록처럼 보이는 허위 콘텐츠를 생성하고, 개인의 사생활과 취약점을 추론하며, 조작된 진실을 만들어낼 수도 있다.
따라서 AI 기반 신뢰 기술은 더 많은 데이터를 소유하는 방향으로 발전해서는 안 된다.
AI 기반 신뢰 기술은 필요한 신호만 안전하게 해석하고, 민감한 원본은 보호하며, 판단의 근거와 한계를 사용자에게 설명하는 방향으로 발전해야 한다.
원본 정보는 보호되어야 한다.
판단값은 설명 가능해야 한다.
기록은 목적에 맞게 제한되어야 한다.

사용자는 자신의 기록에 대한 통제권을 가져야 한다.
검증은 가능해야 하지만, 노출은 최소화되어야 한다.
이것이 기록 사회에서 신뢰 기술이 가야 할 방향이다.
기록은 문명의 기억이다.
그러나 권한 없는 기록은 폭력이 된다.
기록은 악을 막는 방패가 될 수 있다.
그러나 통제되지 않으면 악을 조직하는 칼이 될 수 있다.
따라서 미래의 신뢰 기술은 더 많은 데이터를 모으는 기술이 아니라, 필요한 기록만 안전하게 구조화하고, 필요한 사실만 검증하며, 인간이 스스로를 보호할 수 있도록 돕는 기술이어야 한다.
기록은 통제가 아니라 보호를 위해 존재해야 한다.

기록은 진실 그 자체가 아니라, 인간이 진실에 접근하기 위해 남긴 흔적이다.
그러나 그 흔적은 보는 마음, 사용하는 권한, 공개되는 맥락에 따라 신뢰가 되기도 하고 위험이 되기도 한다.
따라서 기록은 남겨졌다는 이유만으로 정당하지 않고, 공개됐다는 이유만으로 진실도 아니다.
기록의 가치는 그것이 누구를 보호하고, 무엇을 증명하며, 어떤 위험을 줄이는가에 의해 결정된다.
미래의 신뢰 기술은 더 많이 기록하는 기술이 아니라, 흔들리는 인간의 판단 속에서 필요한 사실만 안전하게 검증하게 하는 기술이어야 한다.